

**不安で夜眠れない
AWSアカウント管理者に送る
処方箋という名のハンズオン**


Profile


角山 恵介 (Keisuke Kadoyama)

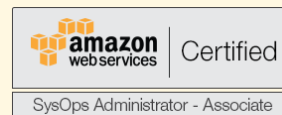
- SI歴 10年
 - エンタープライズ 4年
 - WEB 6年
 - 今年からまたエンタープライズへ
- AWS歴 6年
 - ソリューションアーキテクト
 - Cloud Migration / DevOps / Trouble Shooting



 @bageljp

 kadoyama.keisuke

 bageljp



Questions ?

- とりあえずAWSアカウントを取得したが、そのまま使いはじめて大丈夫なの？
- 最初のシステムが本番稼働しはじめたけど、このまま次々システムを動かして問題はないの？
- なしくずし的にAWSアカウントが増えていってるがこのままで大丈夫？
- AWSアカウントの管理をしているけど不安で夜も眠れないんだけど？

Overview

- AWSアカウントを取得して、最初にやっておくべき初期設定をハンズオン形式で学んでもらう 🔧
- 設定しない場合のリスクを理解してもらう
- セキュリティだけではなく設定しておく便利なTipsも
- ⚠ 今日の手ズオンは1コイン程度の料金が発生します ⚠

Infomation

- 会場のWiFi ⚡

SSID	GOTANDA-MESSE
Password	123412341234

- 本資料のURL <http://bit.ly/jaws2017h1>
- JAWS DAYS全体のハッシュタグ #jawsdays #jawsug
- ワークショップトラックのハッシュタグ #jd2017_workshop

- 1. ルートアカウントの保護**
- 2. IAMユーザーとパスワードポリシー**
- 3. 証跡ログの設定**
- 4. 構成管理の設定**
- 5. Trusted Advisor**
- 6. 請求周りの設定**

Appendix. 複数のAWSアカウント運用Tips

AWSアカウント取得

アカウント周りのハンズオンなので、
すでに本番システムを動作させているAWSアカウントや、
管理者権限を持っていない場合は、新規AWSアカウント取得を推奨

必要なもの

- アカウント作成用のメールアドレスとパスワード
- 認証用のPINコードを受け取るための電話番号
- クレジットカード

手順はこちらを参照

<https://aws.amazon.com/jp/register-flow/>

1. ルートアカウントの保護

2. IAMユーザーとパスワードポリシー

3. 証跡ログの設定

4. 構成管理の設定

5. Trusted Advisor

6. 請求周りの設定

Appendix. 複数のAWSアカウント運用Tips

1. ルートアカウントの保護

Why / Risk

- AWSのすべての操作が可能な**管理者権限**を持つアカウントのため、権限の制限ができない
- ルートアカウントの情報が漏洩して乗っ取られると何でもされてしまう
意図しない課金、既存システムの削除、システムが持つデータや情報の漏洩 🙊

Answer

- パスワードを複雑にする
- MFA (他要素認証) の有効化
- APIキーの削除
 - 不要なAPIキーを悪用されると、ログインしなくてもAWSを**管理者権限**で操作できてしまう
- 普段の操作にはルートアカウントを**使用しない**

1. ルートアカウントの保護

以下のURLアクセスして右上の [サインアップ] をクリック

<https://aws.amazon.com/jp/>



The screenshot shows the AWS Japan homepage. The top navigation bar includes links for 'メニュー' (Menu), 'amazon web services', '開始方法' (Getting Started), '製品' (Products), 'ソリューション' (Solutions), '料金表' (Pricing), and '詳細' (Details). On the right side of the navigation bar, there are links for '日本語' (Japanese), 'アカウント' (Account), and a highlighted 'サインアップ' (Sign Up) button. A red arrow points to the 'サインアップ' button.

Amazon AI を発表
強力な人工知能をすべての開発者に
詳細はこちら ▶

リソース管理を始めましょう
コンソールへサインイン ▶

コンソールモバイルアプリ
iOS、Android デバイスでリソース
チェックができます
詳細・モバイル版ダウンロードはこ
ちら ▶

AWS クラウドの開始方法
わずか数分！AWS の始め方をご紹介

AWS トレーニング 入門シリーズ
無料動画とセルフペースラボで AWS サー
ビスの開始方法を習得


AWS 課金体系・見積り方法のご紹介
料金体系や AWS 見積もりツールのご利用
方法をご紹介

国内のイベント・セミナースケジュール
初心者から上級者まで役立つセミナー・オン
ラインセミナーを毎月開催

製品を調べる

1. ルートアカウントの保護

- ①メールアドレス
- ②パスワードを入力して
- ③[Sign in using our secure server] をクリック



Sign In or Create an AWS Account

What is your email (phone for mobile accounts)?

E-mail or mobile number:

①

☐ I am a new user.

☒ I am a returning user and my password is:


②

③

Sign in using our secure server

[Forgot your password?](#)

Try AWS with a 10-Minute Tutorial



"Hello, World!" technical documents to help you get started with AWS.

[View all tutorials »](#)

Learn more about [AWS Identity and Access Management](#) and [AWS Multi-Factor Authentication](#), features that provide additional security for your AWS Account. View full [AWS Free Usage Tier](#) offer terms.

About Amazon.com Sign In

Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use of this site is governed by our [Terms of Use](#) and [Privacy Policy](#) linked below. Your use of Amazon Web Services products and services is governed by the [AWS Customer Agreement](#) linked below unless you purchase these products and services from an AWS Value Added Reseller.

1. ルートアカウントの保護

AWSサービスの下に表示されているテキストボックスに [IAM] と入力し、表示されたIAMサービスをクリック

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with 'サービス' (Services) and 'リソースグループ' (Resource Groups). Below this, the 'AWS サービス' (AWS Services) section is visible. A search bar contains the text 'IAM'. Below the search bar, a list of services is shown, with 'IAM' (ユーザーアクセスと暗号化キーの管理) highlighted. A red arrow points to the 'IAM' service. To the right, the '注目の次のステップ' (Next steps) section lists 'コストの管理' (Cost management) and 'ベストプラクティスの習得' (Learn best practices). Below that, the '最新情報' (Latest news) section features announcements for 'AWS Batch' and 'Amazon Lightsail'.

サービス リソースグループ

AWS サービス

IAM

ユーザーアクセスと暗号化キーの管理

OpsWorks VPC

すべてのサービス

注目の次のステップ

コストの管理
コストと使用量の予算に基づいてリアルタイムの請求アラートを取得 [今すぐ開始](#)

ベストプラクティスの習得
AWS Trusted Advisor を使用して、セキュリティ、パフォーマンス、コスト、および可用性のベストプラクティスを得る [今すぐ開始](#)

最新情報

AWS Batch のアナウンス
AWS Batch の一般提供開始。AWS Batch を使用することにより、開発者、科学者、およびエンジニアは、大規模なバッチジョブを簡単に処理することができます。 [詳細はこちら](#)

Amazon Lightsail のアナウンス
この新しいサービスを使用して、VPS を AWS で予測可能な低コストで起動および管理できるようになります。 [詳細はこちら](#)

すべて表示

ソリューションの構築
シンプルなウィザードと自動化されたワークフローで作業を開始します。

仮想マシンの起動
EC2 を利用した場合
~1 分

ウェブアプリケーションの作成
Elastic Beanstalk を利用した場合
~6 分

サーバーレスマイクロサービスのデプロイ
Lambda、API Gateway を利用した場合
~2 分

静的ウェブサイトのホスティング
S3、CloudFront、Route 53 を利用した場合
~5 分

モバイルアプリのバックエンドを作成
Mobile Hub を利用した場合
~5 分

ドメインの登録
Route 53 を利用した場合
~3 分

1. ルートアカウントの保護

IAM = Identity and Access Management (無料)

「どのユーザがどのAWSリソースへアクセスできるか」を制御する仕組み
AWSのセキュリティの要

The screenshot displays the AWS IAM console interface. The top navigation bar includes links for Services, Resource Groups, and a user profile. The left sidebar contains a search bar and a list of navigation options: Dashboard, Groups, Users, Roles, Policies, ID Providers, Account Settings, and Authentication Information Report. The main content area is titled 'Identity and Access Management へようこそ' and provides a sign-in link for the IAM user. It also shows summary statistics for IAM resources: 0 Users, 0 Groups, 0 Roles, 0 ID Providers, and 0 Custom Management Policies. A 'Security Status' section features a progress bar and a checklist of five security tasks, with the first task, 'Removal of root access keys', marked as complete. The right-hand panel includes a 'Featured Content' section with a video player for 'Introduction to AWS IAM' and an 'Additional Information' section with links to IAM documentation, Web ID Federation, Policy Simulator, and other resources.

サービス リソースグループ

IAM の検索

Identity and Access Management へようこそ

IAM ユーザーのサインインリンク:
[https://\[redacted\].signin.aws.amazon.com/console](https://[redacted].signin.aws.amazon.com/console) カスタマイズ | リンクのコピー

IAM リソース

ユーザー: 0 ロール: 0
グループ: 0 ID プロバイダ: 0
カスタマー管理ポリシー: 0

セキュリティステータス 5 項目中 1 項目が完了しています。

- ✓ ルートアクセスキーの削除
- ⚠ ルートアカウントの MFA を有効化
- ⚠ 個々の IAM ユーザーの作成
- ⚠ グループを使用してアクセス許可を割り当て
- ⚠ IAM パスワードポリシーの適用

注目の機能

Introduction to AWS IAM

追加情報

IAM ドキュメント
Web ID フェデレーションのプレイグラウンド
Policy Simulator
動画、IAM リリース履歴、および追加のリソース

1. ルートアカウントの保護

一番上の [ルートアクセスキーの削除] でルートアカウントのAPIキーを削除



削除する場合は事前にシステム等で利用していないかよく確認

セキュリティ 認証情報

AWS アカウントの認証情報を管理するには、このページを使用します。AWS Identity and Access Management (IAM) ユーザーの認証情報を管理するには、[IAM コンソール](#)を使用します。

AWS 認証情報の種類と、その使用方法の詳細は、「AWS General Reference」の「[AWS Security Credentials](#)」を参照してください。

作成日	削除済み	アクセスキー ID	前回使用したもの	前回使用したリージョン	前回使用したサービス	ステータス	アクション
4月 27 2012		AKIAI44QH8DHBVS72L236	該当なし	N/A	N/A	有効	無効化 削除

注: 一度に持つことができるのは、最大 2 つのアクセスキー（有効または無効）です。

[新しいアクセスキーの作成](#)

1. ルートアカウントの保護

[ルートアカウントのMFAを有効化] をクリックし、
[MFAの管理] をクリック

The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links: IAM の検索, ダッシュボード, グループ, ユーザー, ロール, ポリシー, ID プロバイダー, アカウント設定, 認証情報レポート, and 暗号化キー. The main content area is titled 'Identity and Access Management へようこそ'. It displays the IAM user's sign-in link, IAM resources (0 users, 0 roles, 0 groups, 0 ID providers, 0 custom management policies), and a security status bar indicating 1 of 5 items is complete. A list of security warnings is shown, with 'Root account MFA' highlighted by a red box. Below this warning, the 'MFA の管理' link is also highlighted by a red box and pointed to by a red arrow. The right sidebar features '注目機能' (Featured) with a video player for 'Introduction to AWS IAM' and '追加情報' (Additional Information) with links to IAM documents, Web ID federation, Policy Simulator, and other resources.

1. ルートアカウントの保護

MFAとは？

MFA = Multi Factor Authentication

要はパスワード+αによる2段階認証 (6桁の認証コード)

仮想MFAデバイス

- Android / iOSアプリ: Authenticator / Authy
- Chrome Extension: [Authenticator](#)
- Firefox Extension: [Open Two-Factor Authenticator](#)

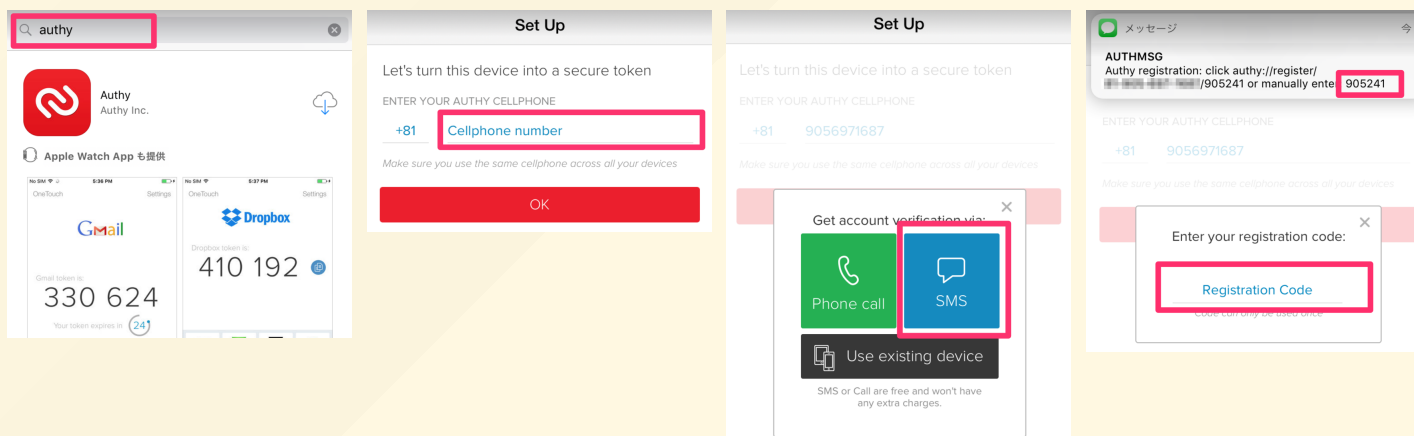
ハードウェアMFAデバイス



1. ルートアカウントの保護

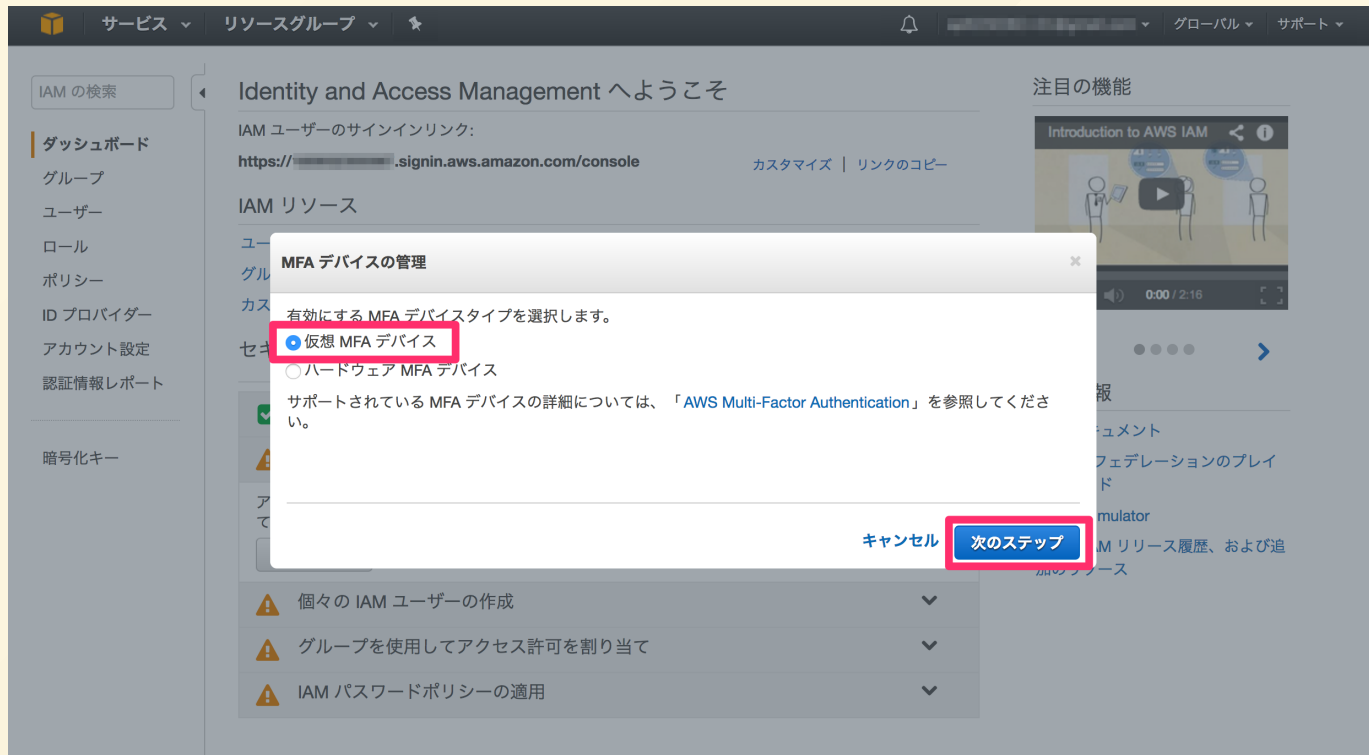
仮想MFAデバイスをお持ちでない方

Android / iOSスマートフォンをお持ちの方はアプリのストアより「Authy」と検索してアプリをダウンロード
起動してSMSで電話番号の認証をすませる



1. ルートアカウントの保護

[仮想MFAデバイス] を選択する



1. ルートアカウントの保護

QRコードが表示されるので、仮想MFAデバイスのアプリからスキャンする



Authyをお使いの方は [+] ボタンから [Scan QR Code] をタップして表示されているQRコードをスキャン



1. ルートアカウントの保護

仮想MFAデバイスに表示される認証コードを2つ入力して有効化
※2つの認証コードは異なるコードであること



MFA デバイスの管理

仮想 MFA アプリケーションが QR コードのスキャンをサポートしている場合は、スマートフォンのカメラで次の画像をスキャンします。



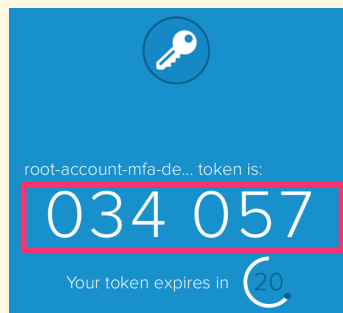
▶ 手動設定のシークレットキーを表示
アプリケーションを設定したら、下のボックスに 2 つの連続する認証コードを入力し、[仮想 MFA の有効化] をクリックします。

認証コード 1

認証コード 2

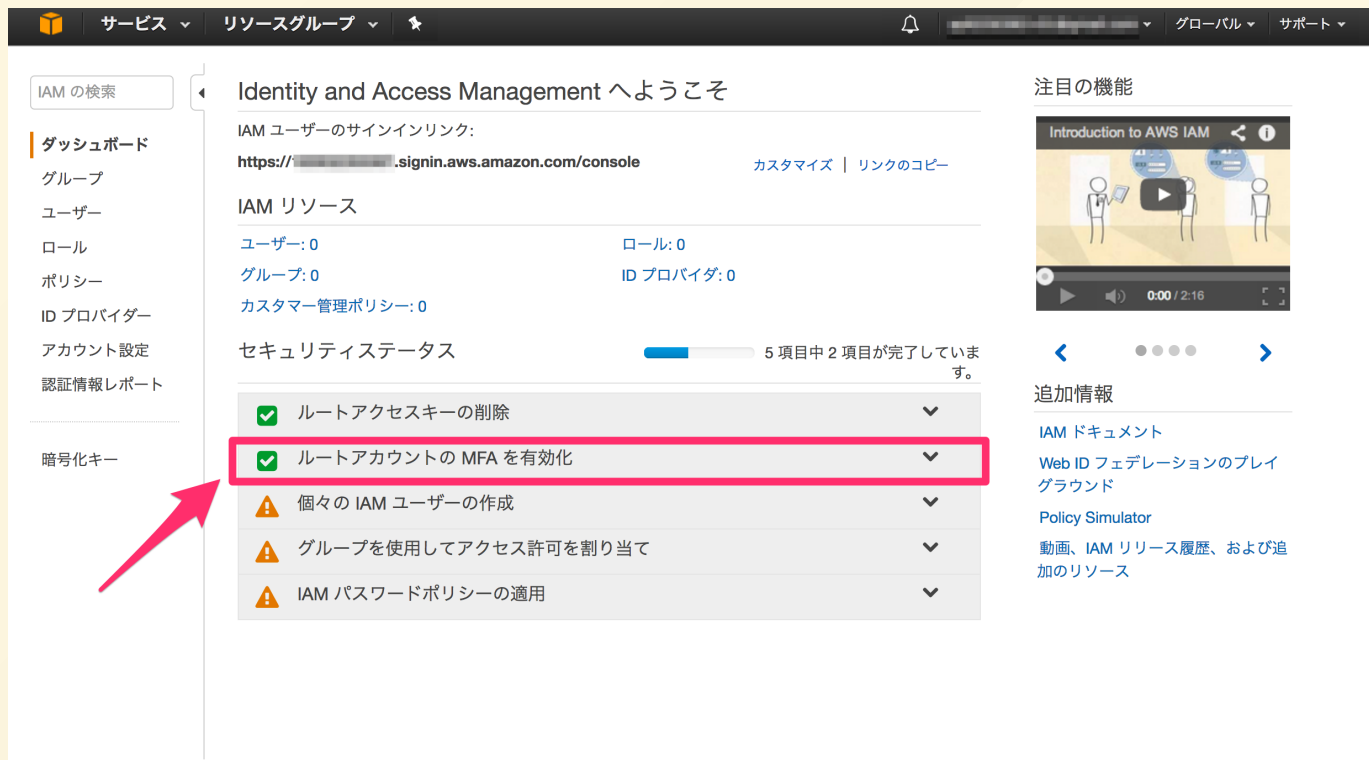
キャンセル 戻る 仮想 MFA の有効化

Authyをお使いの方は以下の画面に表示される6桁の認証コードを入力



1. ルートアカウントの保護

無事ルートアカウントのMFAが有効になりました



The screenshot shows the AWS IAM console interface. The left sidebar contains a navigation menu with the following items: **ダッシュボード**, グループ, ユーザー, ロール, ポリシー, ID プロバイダー, アカウント設定, 認証情報レポート, and 暗号化キー. The main content area is titled 'Identity and Access Management へようこそ'. It displays the IAM user sign-in link, IAM resources (0 users, 0 groups, 0 roles, 0 ID providers, 0 custom management policies), and a 'Security Status' section. The 'Security Status' section shows a progress bar for 5 items, with 2 completed. The items are:

- ✓ ルートアクセスキーの削除
- ✓ ルートアカウントの MFA を有効化 (highlighted with a red box)
- ⚠ 個々の IAM ユーザーの作成
- ⚠ グループを使用してアクセス許可を割り当て
- ⚠ IAM パスワードポリシーの適用

1. ルートアカウントの保護

確認のため一度サインアウトし、

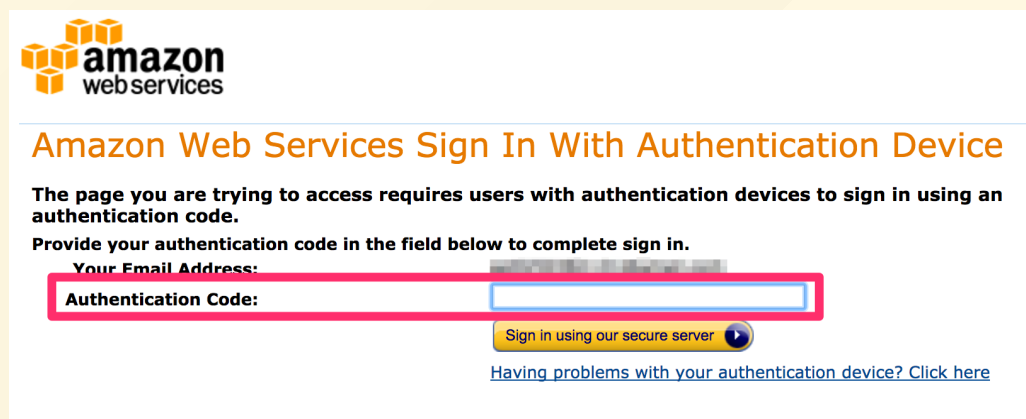


もう一度サインイン



1. ルートアカウントの保護

メールアドレス、パスワードを入力後、登録した仮想MFAデバイスの認証コードが求められる



The screenshot shows the Amazon Web Services login page for users with authentication devices. It includes the Amazon Web Services logo, a title, instructions, input fields for email and authentication code, a sign-in button, and a link for troubleshooting.

amazon
web services


Amazon Web Services Sign In With Authentication Device

The page you are trying to access requires users with authentication devices to sign in using an authentication code.

Provide your authentication code in the field below to complete sign in.

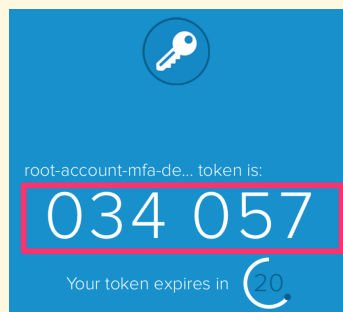
Your Email Address:

Authentication Code:

Sign in using our secure server 

[Having problems with your authentication device? Click here](#)

Authyをお使いの方は以下の画面に表示される6桁の認証コードを入力



1. ルートアカウントの保護

Why / Risk

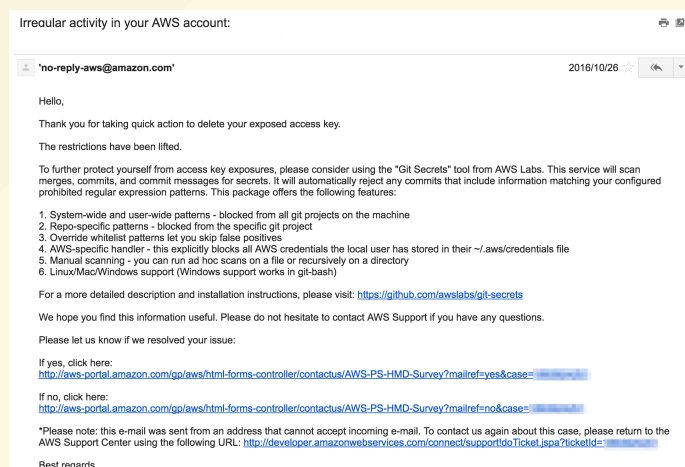
- AWSのすべての操作が可能な**管理者権限**を持つアカウントのため、権限の制限ができない
- ルートアカウントの情報が漏洩して乗っ取られると何でもされてしまう
意図しない課金、既存システムの削除、システムが持つデータや情報の漏洩 🙊

Answer

- パスワードを複雑にする
- MFA (他要素認証) の有効化
- APIキーの削除
 - 不要なAPIキーを悪用されると、ログインしなくてもAWSを**管理者権限**で操作できてしまう
- 普段の操作にはルートアカウントを**使用しない**

Break

- 不要なAPIキーの作成や、不適切な権限が付与されているかだけでなく、誤ってAPIキーがグローバルに公開されていないかチェック
 - Amazonが公開しているgit-secretsというツールで、プログラムのgitリポジトリにAPIキーをcommitしていないかチェック
<https://github.com/awslabs/git-secrets>
 - もしグローバル公開したり漏洩の危険性がある場合、Amazonから警告メールが来ることも
※AWSアカウントへのアクセスが強制停止されることもあります



1. ルートアカウントの保護

2. IAMユーザーとパスワードポリシー

3. 証跡ログの設定

4. 構成管理の設定

5. Trusted Advisor

6. 請求周りの設定

Appendix. 複数のAWSアカウント運用Tips

2. IAMユーザとパスワードポリシー

Why / Risk

- 管理者権限を持ったルートアカウントの代わりに他のアカウントが必要
- 漏洩時や操作ミスを考慮してアカウントには適切な権限管理を行いたい
- アカウントを共有していると誰が何をしたかの証跡が追いつらい

Answer

- IAMユーザと、権限を定義したIAMポリシーを作成
 - IAMユーザは共有せずに利用者単位で作成
 - 権限はIAMユーザではなくIAMグループに設定してIAMユーザの権限管理を楽にする
- IAMユーザでもMFAを有効化
- パスワードポリシーを設定して簡単なパスワードを設定できないように

2. IAMユーザとパスワードポリシー

IAMの画面を表示し、末尾の [IAMパスワードポリシーの適用] から [パスワードポリシーの管理] をクリック

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like 'ダッシュボード', 'グループ', 'ユーザー', 'ロール', 'ポリシー', 'ID プロバイダー', 'アカウント設定', '認証情報レポート', and '暗号化キー'. The main content area is titled 'Identity and Access Management へようこそ'. It displays the IAM user sign-in link, resource counts (0 users, 0 roles, 0 groups, 0 ID providers, 0 customer managed policies), and a security status bar indicating 2 out of 5 items are complete. A list of security tasks follows, with 'IAM パスワードポリシーの適用' (IAM Password Policy Application) highlighted by a red box. Below this, a description states that password policies are used to require strong passwords and periodic rotation. At the bottom of this section, the button 'パスワードポリシーの管理' (Manage Password Policy) is also highlighted with a red box. On the right side of the console, there is a '注目の機能' (Featured) section with a video player and an '追加情報' (Additional Information) section with links to IAM documentation, Web ID Federation, Policy Simulator, and a video about IAM releases.

2. IAMユーザとパスワードポリシー

パスワードポリシーを設定して [パスワードポリシーの適用] をクリック

サービス リソースグループ

パスワードポリシー

パスワードポリシーは、IAM ユーザーが設定できるパスワードの種類を定義するルールのセットです。パスワードポリシーの詳細については、「IAM の使用」の「[パスワードの管理](#)」を参照してください。

現在、この AWS アカウントにパスワードポリシーはありません。以下のパスワードポリシーを指定します。

パスワードの最小長: 8

- ☒ 少なくとも 1 つの大文字が必要 ⓘ
- ☒ 少なくとも 1 つの小文字が必要 ⓘ
- ☒ 少なくとも 1 つの数字が必要 ⓘ
- ☒ 少なくとも 1 つの英数字以外の文字が必要 ⓘ
- ☒ ユーザーにパスワードの変更を許可 ⓘ
- ☐ パスワードの失効を許可 ⓘ
- パスワードの有効期間 (日数):
- ☐ パスワードの再利用を禁止 ⓘ
- 記憶するパスワードの数:
- ☐ パスワードの有効期限で管理者のリセットが必要 ⓘ

パスワードポリシーの適用

パスワードポリシーの削除

2. IAMユーザーとパスワードポリシー

左メニューから [ユーザー] をクリック



[ユーザーを追加] をクリック



2. IAMユーザとパスワードポリシー

ユーザーを追加

1

2

3

4

詳細

アクセス権限

確認

完了

ユーザー詳細の設定

同じアクセスの種類とアクセス権限を使用して複数のユーザーを一度に追加できます。 [詳細はこちら](#)

ユーザー名*

①

別のユーザーの追加

AWS アクセスの種類を選択

これらのユーザーから AWS にアクセスする方法を選択します。アクセスキーと自動生成パスワードは前のステップで提供されています。 [詳細はこちら](#)

アクセスの種類*

☐ プログラムによるアクセス

AWS API、CLI、SDK などの開発ツールの **アクセスキー ID** と **シークレットアクセスキー** を有効にします。

☒ **AWS マネジメントコンソールへのアクセス** ②

ユーザーに AWS マネジメントコンソールへのサインインを許可するための **パスワード** を有効にします。

コンソールのパスワード*

☒ 自動生成パスワード ③

☐ カスタムパスワード

パスワードのリセットが必要

☒ ユーザーは次回のサインインで新しいパスワードを作成する必要があります ④

⑤

* 必須

キャンセル

次のステップ: アクセス権限

2. IAMユーザとパスワードポリシー

IAMグループを使って権限制御を行うため [グループの作成] をクリック

ユーザーを追加

1 2 3 4
詳細 アクセス権限 確認 完了

のアクセス権限を設定

ユーザーをグループに追加

アクセス権限を既存のユーザーからコピー

既存のポリシーを直接アタッチ

グループの開始方法
グループをまだ作成していません。ユーザーのアクセス権限は、グループを使ってジョブ機能、AWS サービスへのアクセス、カスタムのアクセス権限別に管理するのが最善の方法です。グループを作成して開始してください。 [詳細はこちら](#)

グループの作成

キャンセル 戻る 次のステップ: 確認

2. IAMユーザとパスワードポリシー

グループ名を入力し、[AdministratorAccess] ポリシーを選択して作成する

グループの作成

グループを作成して、そのグループにアタッチするポリシーを選択します。ユーザーのアクセス権限は、グループを使ってジョブ機能、AWS サービスへのアクセス、カスタムのアクセス権限別に管理するのが最善の方法です。 [詳細はこちら](#)

グループ名

ポリシーの作成

更新

フィルター: ポリシータイプ

10 件の結果を表示しています

	ポリシー名	タイプ	添付ファイル	説明
<input type="checkbox"/>	DatabaseAdministrator	ジョブ機能	0	Grants full access permissions to AWS services and actions r...
<input type="checkbox"/>	ServiceCatalogAdminFullAcc...	AWS による管理	0	Provides full access to the service catalog admin console.
<input type="checkbox"/>	SystemAdministrator	ジョブ機能	0	Grants full access permissions necessary for resources requi...
<input checked="" type="checkbox"/>	AdministratorAccess	ジョブ機能	0	Provides full access to AWS services and resources.
<input type="checkbox"/>	AmazonWorkSpacesAdmin	AWS による管理	0	Provides access to Amazon WorkSpaces administrative actio...
<input type="checkbox"/>	AmazonAPIGatewayAdminist...	AWS による管理	0	Provides full access to create/edit/delete APIs in Amazon API...
<input type="checkbox"/>	ServiceCatalogAdminReadOn...	AWS による管理	0	Provides read only access to the service catalog admin cons...
<input type="checkbox"/>	NetworkAdministrator	ジョブ機能	0	Grants full access permissions to AWS services and actions r...
<input type="checkbox"/>	AmazonWorkSpacesApplicat...	AWS による管理	0	Provides administrator access for packaging an application i...

キャンセル

グループの作成

2. IAMユーザとパスワードポリシー

作成したIAMグループにチェックが入っていることを確認し、次へ

ユーザーを追加

1 詳細 2 アクセス権限 3 確認 4 完了

ユーザーのアクセス権限を設定

ユーザーをグループに追加

アクセス権限を既存のユーザーからコピー

既存のポリシーを直接アタッチ

ユーザーを既存のグループに追加するか、新しいグループを作成します。ユーザーのアクセス権限は、グループを使ってジョブ機能別に管理するのが最善の方法です。 [詳細はこちら](#)

グループの作成 更新

検索

1件の結果を表示しています

グループ	アタッチされたポリシー
<input checked="" type="checkbox"/>	AdministratorAccess

2. IAMユーザとパスワードポリシー

内容を確認し、[ユーザーの作成] をクリック

ユーザーを追加

1 2 3 4
詳細 アクセス権限 確認 完了

確認

選択内容を確認します。ユーザーを作成した後で、自動生成パスワードとアクセスキーを確認してダウンロードできます。

ユーザー詳細

ユーザー名	
AWS アクセスの種類	AWS マネジメントコンソールへのアクセス - パスワードを使用
コンソールのパスワードの種類	自動生成
パスワードのリセットが必要	はい

アクセス権限の概要

上記のユーザーは、次のグループに追加されます。

タイプ	名前
グループ	

キャンセル 戻る **ユーザーの作成**

2. IAMユーザとパスワードポリシー

- ①サインイン用のURL、②パスワードをメモするか、
- ③Eメールでログイン情報を送信する

The screenshot shows the 'Add User' wizard in the AWS IAM console. The progress bar at the top indicates four steps: 1. Details, 2. Access permissions, 3. Confirmation, and 4. Completed. The main content area shows a success message with a green checkmark. Below the message, there is a link to the sign-in URL, which is highlighted with a red box and a circled 1. Below the link, there is a table with three columns: 'User', 'Password', and 'Send login instructions by email'. The 'User' column contains a green checkmark and a user name. The 'Password' column contains a password field with a red box around the 'Show' button and a circled 2. The 'Send login instructions by email' column contains a blue link 'Send email' with a red box around it and a circled 3. At the bottom right, there is a 'Close' button.

ユーザーを追加

1 詳細 2 アクセス権限 3 確認 4 完了

成功

以下に示すユーザーを正常に作成しました。ユーザーのセキュリティ認証情報を確認してダウンロードできます。AWS マネジメントコンソールへのサインイン手順を E メールでユーザーに送信することもできます。今回が、これらの認証情報をダウンロードできる最後の機会です。ただし、新しい認証情報はいつでも作成できます。

AWS マネジメントコンソールへのアクセス権を持つユーザーは [https://\[redacted\].signin.aws.amazon.com/console](https://[redacted].signin.aws.amazon.com/console) でサインインできます

①

.csv のダウンロード

ユーザー	パスワード	ログイン手順を E メールで送信
▶ ✓ [redacted]	② ***** 表示	③ Eメールの送信 🔗

閉じる

2. IAMユーザとパスワードポリシー

IAMユーザーもMFAを有効にする

左メニューの [ユーザー] から作成したIAMユーザーの名前をクリック



The screenshot shows the AWS IAM console interface. On the left sidebar, the 'ユーザー' (Users) link is highlighted with a red box. The main content area displays a table of IAM users. The first user, 'root', is highlighted with a red box. The table columns include 'ユーザー名' (User name), 'グループ' (Group), 'パスワード' (Password), '最終サインイン' (Last sign-in), 'アクセスキー' (Access key), and '作成時刻' (Created at).

ユーザー名	グループ	パスワード	最終サインイン	アクセスキー	作成時刻
root	1	該当なし	なし	2017-03-05 18:12 UTC+0900	

2. IAMユーザとパスワードポリシー

- ① [認証情報] タブを選択し、
- ② [MFAデバイスの割り当て] をクリック



先ほどのルートアカウントの手順と同様の手順で、
仮想MFAデバイスを有効にする

2. IAMユーザとパスワードポリシー

ここまでできたらルートアカウントの使用をやめるためサインアウトし、



IAMユーザーのサインイン用URLにアクセスする

<https://xxxxxxxxxxxxx.signin.aws.amazon.com>

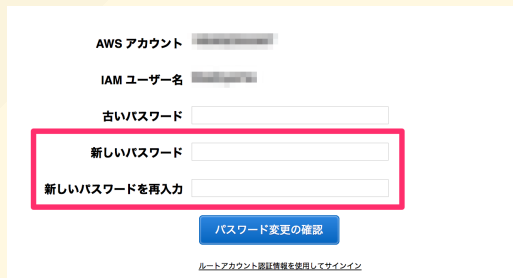
A screenshot of the AWS IAM sign-in page. The page has the 'amazon web services' logo at the top. Below the logo, there are three input fields: 'アカウント:', 'ユーザー名:', and 'パスワード:'. These fields are grouped by a red box. Below the input fields, there is a blue button labeled 'サインイン'. Below the button, there is a note: 'MFA ユーザーは、次の画面でコードを入力してください。' and a link: 'ルートアカウント認証情報を使用してサインイン'.

2. IAMユーザとパスワードポリシー

パスワードを入力するとMFAコードを求められ、



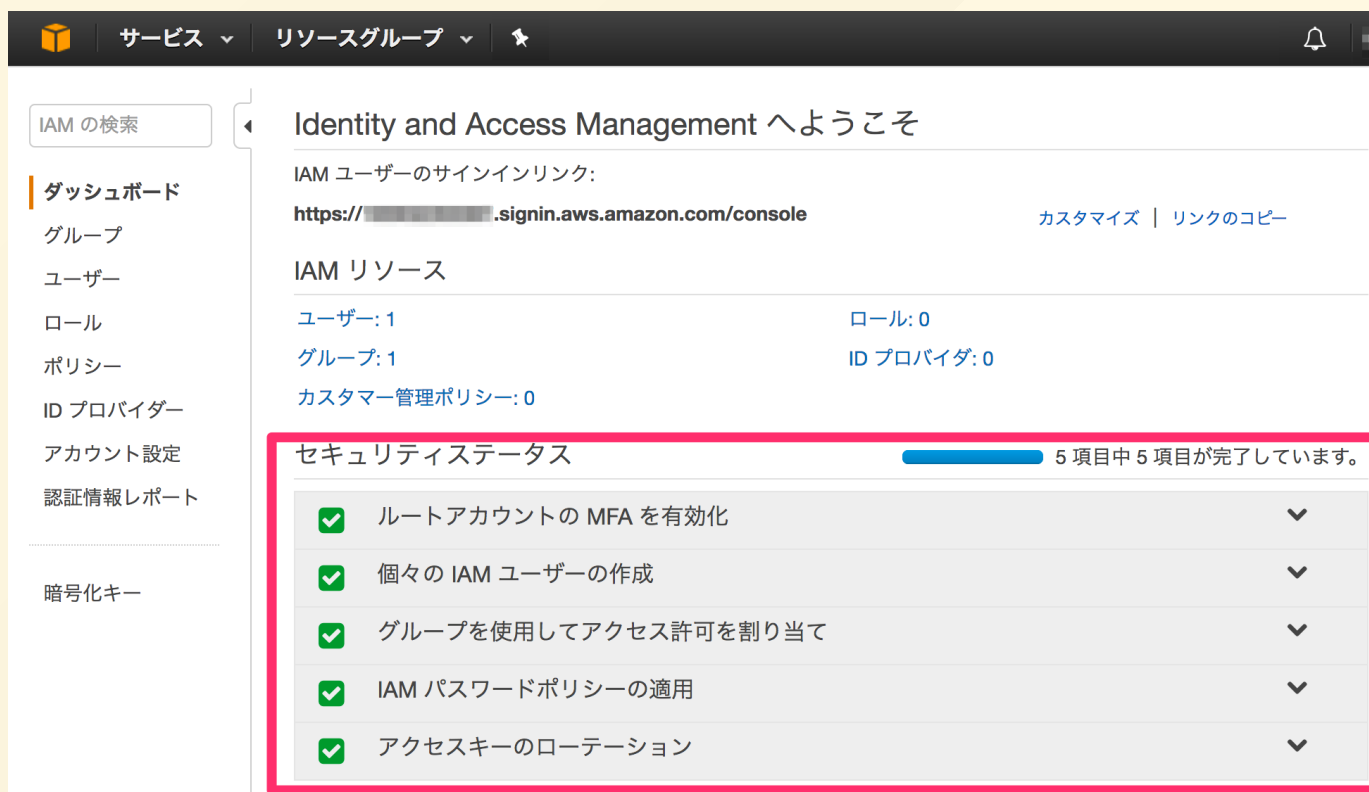
サインインに成功すると強制的に新しいパスワードの設定を求められる



2. IAMユーザとパスワードポリシー

ここまで出来たらセキュリティステータスを確認

<https://console.aws.amazon.com/iam/home>



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links: ダッシュボード, グループ, ユーザー, ロール, ポリシー, ID プロバイダー, アカウント設定, 認証情報レポート, and 暗号化キー. The main content area is titled "Identity and Access Management へようこそ". It displays the IAM user sign-in link, IAM resources (1 user, 1 group, 0 roles, 0 ID providers, 0 custom management policies), and the "セキュリティステータス" (Security Status) section. The Security Status section is highlighted with a red box and shows a progress bar indicating that all 5 items are completed. The items are: ルートアカウントの MFA を有効化, 個々の IAM ユーザーの作成, グループを使用してアクセス許可を割り当て, IAM パスワードポリシーの適用, and アクセスキーのローテーション.

Identity and Access Management へようこそ

IAM ユーザーのサインインリンク:
[https://\[redacted\].signin.aws.amazon.com/console](https://[redacted].signin.aws.amazon.com/console) [カスタマイズ](#) | [リンクのコピー](#)

IAM リソース

ユーザー: 1 ロール: 0
グループ: 1 ID プロバイダ: 0
カスタマー管理ポリシー: 0

セキュリティステータス 5 項目中 5 項目が完了しています。

- ✓ ルートアカウントの MFA を有効化
- ✓ 個々の IAM ユーザーの作成
- ✓ グループを使用してアクセス許可を割り当て
- ✓ IAM パスワードポリシーの適用
- ✓ アクセスキーのローテーション

2. IAMユーザとパスワードポリシー

Why / Risk

- 管理者権限を持ったルートアカウントの代わりに他のアカウントが必要
- 漏洩時や操作ミスを考慮してアカウントには適切な権限管理を行いたい
- アカウントを共有していると誰が何をしたかの証跡が追いつらい

Answer

- IAMユーザーと、権限を定義したIAMポリシーを作成
 - IAMユーザーは共有せずに利用者単位で作成
 - 権限はIAMユーザーではなくIAMグループに設定してIAMユーザーの権限管理を楽にする
- IAMユーザーでもMFAを有効化
- パスワードポリシーを設定して簡単なパスワードを設定できないように

Break

- IAMユーザーのサインイン用URL (アカウント番号) は任意の文字列に変更することが可能

<https://xxxxxxxxxxxxx.signin.aws.amazon.com> ➡ <https://jawsdays.signin.aws.amazon.com>



- IAMユーザーの利用者本人にMFAを設定してもらうには、こちらの公式チュートリアルを参考にIAMポリシーを設定する

http://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/tutorial_users-self-manage-mfa-and-creds.html

1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
- 3. 証跡ログの設定**
4. 構成管理の設定
5. Trusted Advisor
6. 請求周りの設定

Appendix. 複数のAWSアカウント運用Tips

3. 証跡ログの設定

Why / Risk

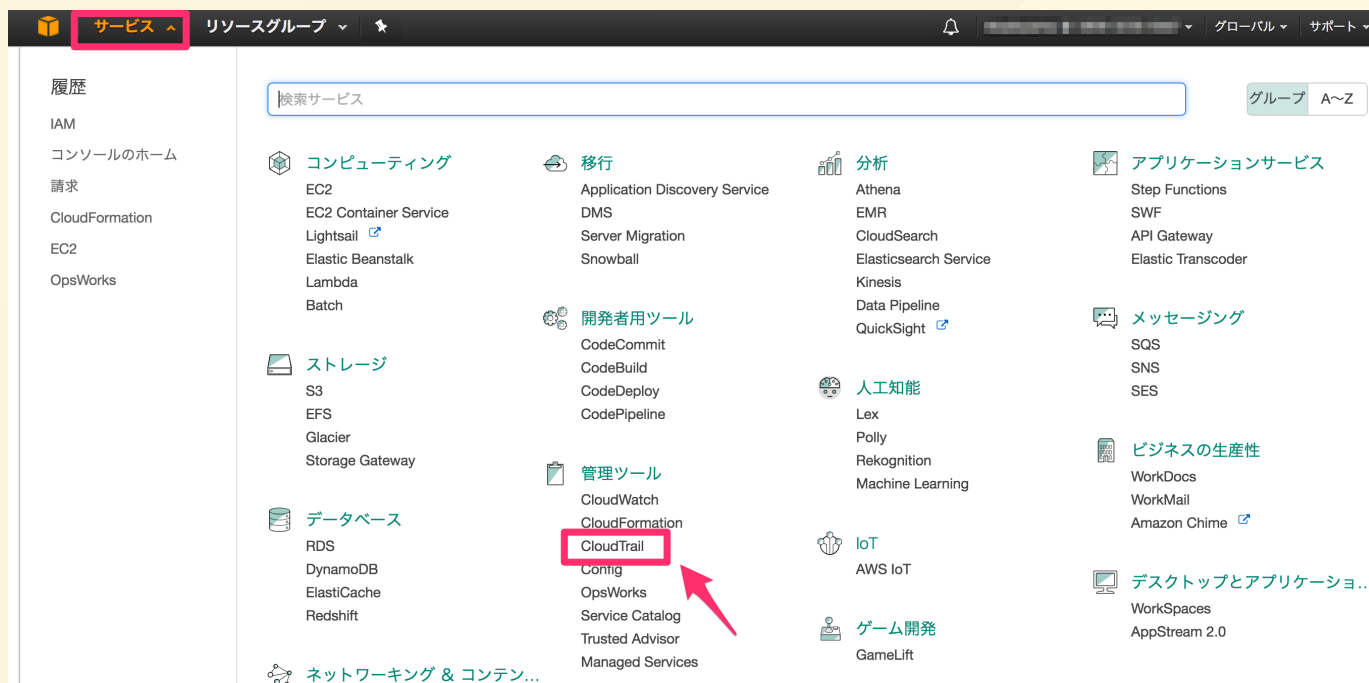
- どの操作を誰が行ったのかわからない
- 悪意のある内部犯行があった場合に犯人がわからない 😈
- 高額なリソースをこっそり使われても誰が利用したのかわからない 🕵️

Answer

- CloudTrailの有効化
 - 管理コンソールやAPIによる操作を証跡ログとして記録する
 - CloudTrailは最初の1つだけなら無料
 - ログを保存するS3のストレージ料金が別途発生
- 利用していないリージョンでも不正利用を記録できるように有効に
- 制限ではなく、あくまで抑止力 ⚠️

3. 証跡ログの設定

左上の [サービス] から [CloudTrail] をクリック



3. 証跡ログの設定

右上のリージョン選択で[東京]リージョンを選択
[今すぐ始める]をクリック



3. 証跡ログの設定

- ①証跡名は好きな名前を、
- ②認証情報は全てのリージョンに適用する、
- ③④証跡ログを保存するS3バケットは新規で作成

サービス リソースグループ

CloudTrail の料金はどのように設定されているか？
CloudTrail のイベント処理は 1 つまでの証跡による処理は無料です。追加の証跡によるイベント処理には料金が発生します。詳細については、次を参照してください。 [料金表](#)。

CloudTrail の有効化

証跡名*

①

証跡情報を全てのリージョンに適用

はい

いいえ

②

新しい S3 バケットを作成しますか

はい

いいえ

③

S3 バケット*

④

詳細

* 必須のフィールド

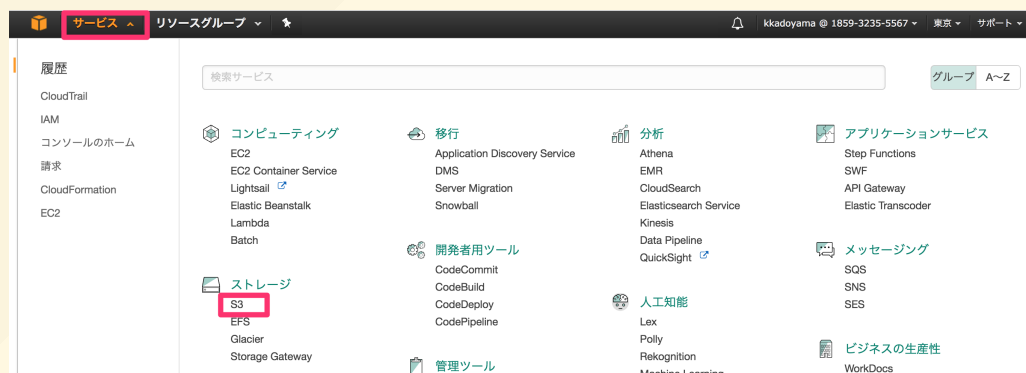
有効化

3. 証跡ログの設定

設定完了



S3に出力されたログ



3. 証跡ログの設定

CloudTrailの証跡ログが出力されているS3バケット



JSON形式で圧縮して保存されている



3. 証跡ログの設定

Why / Risk

- どの操作を誰が行ったのかわからない
- 悪意のある内部犯行があった場合に犯人がわからない 😈
- 高額なリソースをこっそり使われても誰が利用したのかわからない 🕵️

Answer

- CloudTrailの有効化
 - 管理コンソールやAPIによる操作を証跡ログとして記録する
 - CloudTrailは最初の1つだけなら無料
 - ログを保存するS3のストレージ料金が別途発生
- 利用していないリージョンでも不正利用を記録できるように有効に
- 制限ではなく、あくまで抑止力 ⚠️

Break

- CloudWatch LogsやSNSなどAWSの他サービスと連携させることで、ただログを記録するだけでなく、「特定のリソースが削除された」、「ルートアカウントでログインが発生した」など特定のイベントを元にメール通知などが可能
- 証跡ログはJSON形式で保存され、他のログ可視化サービスと連携することでもっと見やすく管理することが可能
 - Splunk
 - Graylog
 - CloudCheckr
 - DataDog
 - etc...

<https://aws.amazon.com/jp/cloudtrail/partners/>

1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
- 4. 構成管理の設定**
5. Trusted Advisor
6. 請求周りの設定

Appendix. 複数のAWSアカウント運用Tips

4. 構成管理の設定

Why / Risk

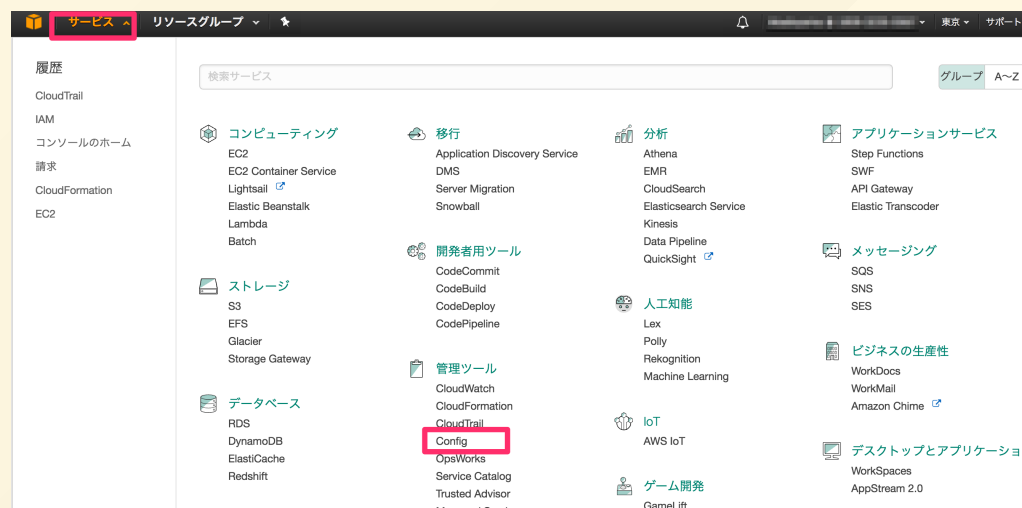
- いつ誰が何をしたか、はCloudTrailの証跡ログから追えるが、そのときAWSのリソースが**どういう状態**だったかわからない
 - 一応証跡ログを順番に追っていけば再現できなくはない... 😊
- 昨年の年末セール対応ってサーバ何台用意してましたっけ？
 - ドキュメントには20台ってあるけど、当日増やした気が...

Answer

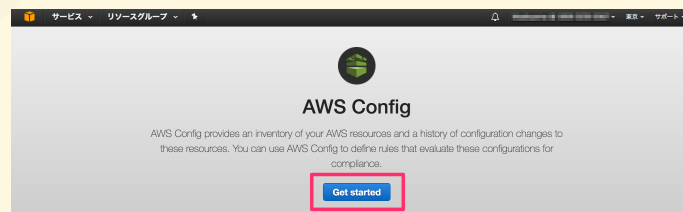
- **AWS Config**の有効化
 - AWSリソースの状態や、各リソースのRelationship (関係) を記録
 - イベントの前後でAWSのリソースが**どう変化したか**記録
 - ルールを定義してルールに沿った設定がされているか自動チェック
 - すべてのAWSサービスの状態を記録してくれるわけではない ⚠

4. 構成管理の設定

左上の [サービス] から [Config] をクリック



[Get started] をクリック



4. 構成管理の設定

- ①[Include global resource] にチェック
- ②構成管理ログを保存するS3バケットは新規で作成

Set up AWS Config

Step 1: Settings

Step 2: AWS Config rules

Step 3: Review

Settings

Specify the types of AWS resources you want AWS Config to record, the Amazon S3 bucket to which it sends files, and the Amazon SNS topic to which it sends notifications. Review the [pricing page](#) before you start.

Resource types to record

Select the types of AWS resources for which you want AWS Config to record configuration changes. By default, AWS Config records configuration changes for all supported resources. You can also choose to record configuration changes for supported global resources in this region.

All resources

- ☒ Record all resources supported in this region ⓘ
- ☒ Include global resources (e.g., AWS IAM resources) ⓘ ①

Specific types

Amazon S3 bucket*

Your bucket receives configuration history and configuration snapshot files, which contain details for the resources that AWS Config records.

- ☒ Create a bucket
- ☐ Choose a bucket from your account
- ☐ Choose a bucket from another account ⓘ

Bucket name* config-bucket- / Prefix (optional) / AWSLogs/ /Config/ap-northeast-1 ②

4. 構成管理の設定

- ③ SNS Topicを設定することで構成に変化があった際に通知できる
- ④ Config roleはAWS Configが利用するIAMロール (権限) の設定
いずれもデフォルト値のまま [Next]

Step 3: Review

Amazon SNS topic

☒ Stream configuration changes and notifications to an Amazon SNS topic.

☒ Create a topic

☐ Choose a topic from your account

☐ Choose a topic from another account ⓘ

Topic name*

AWS Config role*

Grant AWS Config read-only access to your AWS resources so that it can record configuration information, and grant it permission to send this information to Amazon S3 and Amazon SNS.

☒ Create a role

☐ Choose a role from your account

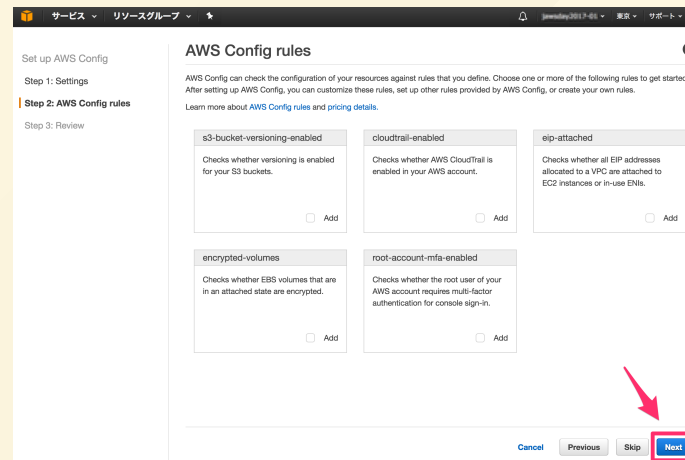
Role name*

* Required

Cancel **Next**

4. 構成管理の設定

AWS Configは構成管理の記録だけでなく、特定のルールに沿った設定が行われているかチェックが可能
今回はとくにチェックを入れず [Next]



自分たちの運用ルールに沿ったルールを設定 (カスタムルールの作成も可能)

- EBSは必ず暗号化する
- S3は必ずバージョニングを有効にする
- ルートアカウントは必ずMFAを有効にする
- RDSのバックアップを有効にする

4. 構成管理の設定

内容を確認して [Confirm]

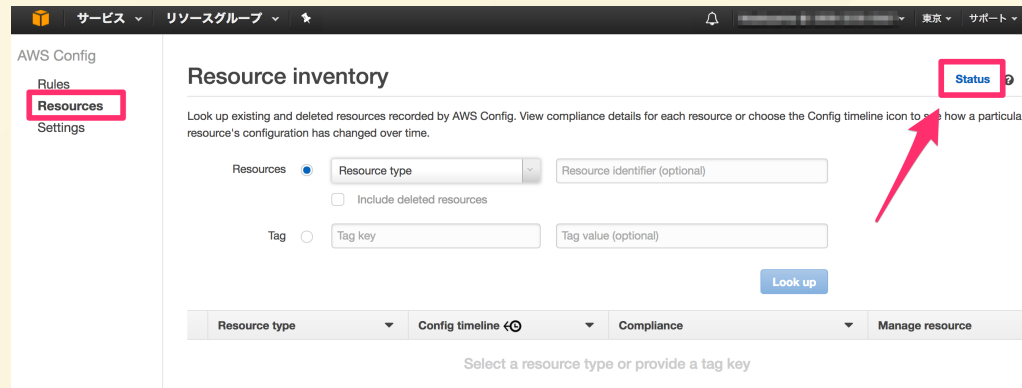
The screenshot shows the AWS Config console during the 'Review' step of setup. The left sidebar lists the steps: 'Set up AWS Config', 'Step 1: Settings', 'Step 2: AWS Config rules', and 'Step 3: Review' (which is highlighted). The main content area is titled 'Review' and contains the following sections:

- Review your AWS Config setup details.** A message stating: "Review your AWS Config setup details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up AWS Config."
- AWS Config rules (2)** A section with two rules:
 - cloudtrail-enabled**: Checks whether AWS CloudTrail is enabled in your AWS account. Optionally, you can specify which S3 bucket, SNS topic, and Amazon CloudWatch Logs ARN to use.
 - root-account-mfa-enabled**: Checks whether the root user of your AWS account requires multi-factor authentication for console sign-in.
- Settings** A section with three settings:
 - Resource types**: All resources (including global resources)
 - Amazon S3 bucket**: config-bucket-[redacted]
 - Amazon SNS topic**: config-topic
 - AWS Config role**: config-role-ap-northeast-1

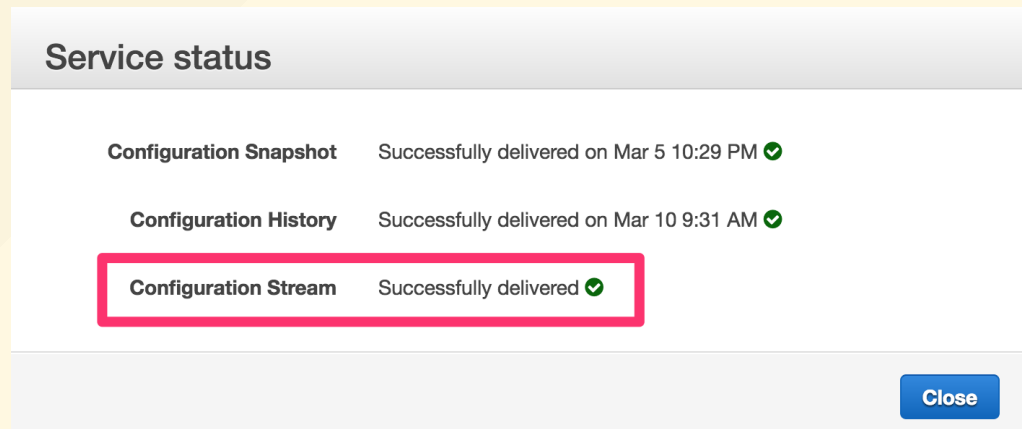
At the bottom right, there are three buttons: 'Cancel', 'Previous', and 'Confirm'. The 'Confirm' button is highlighted with a red rectangular box.

4. 構成管理の設定

左メニューの [Resources] をクリックして [Status] をクリック



[Configuration Stream] がSuccessfullyになっていればOK
あとは勝手にリソース情報を収集して記録していく



4. 構成管理の設定

[Resources] で表示したいAWSリソースを選択して [Look up]

Resource inventory Status ⓘ

Look up existing and deleted resources recorded by AWS Config. View compliance details for each resource or choose the Config timeline icon to see how a particular resource's configuration has changed over time.

Resources ☒ **EC2: Instance**

Tag ☐ **Look up**

Resource type ☐ ACM ☐ Certificate ☐ CloudTrail ☐ Trail ☐ EC2 ☐ CustomerGateway ☐ EIP ☐ Host ☒ **Instance** ☐ InternetGateway ☐ NetworkAcl

Compliance ☐ Manage resource

Resource type or provide a tag key

該当するAWSリソースが一覧に表示される

Resources ☒ **Resource type**

☐ Include deleted resources

Tag ☐ **Look up**

Choose Config timeline ⓘ to view a history of configuration details for the resource.

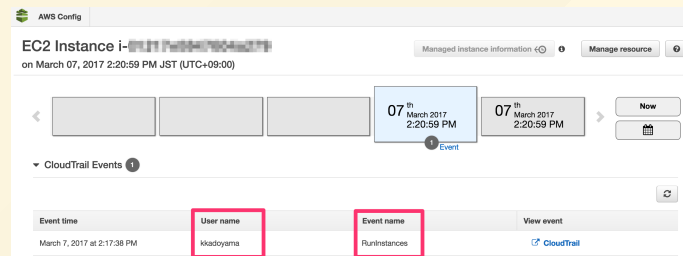
Resource type ☐ Config timeline ⓘ ☐ Compliance ☐ Manage resource

EC2 Instance	i-01217e5947604a279	--	↗
--------------	---------------------	----	-------------------

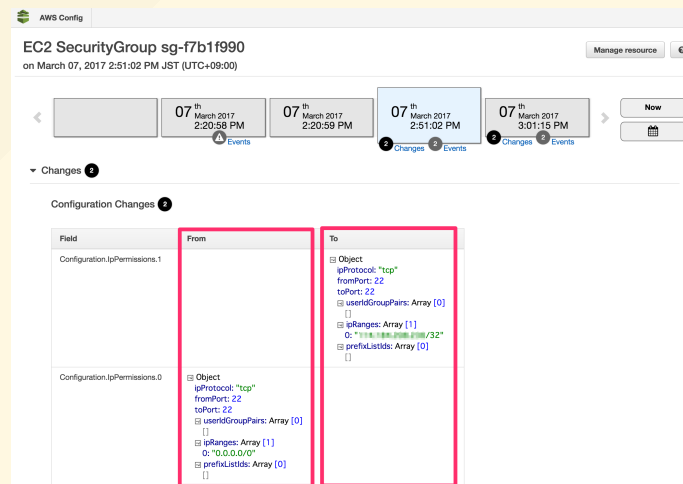
4. 構成管理の設定

イベント発生時刻や内容、前後でリソースの状態がどうなったかが記録

- EC2の作成イベント



- SecurityGroupの変更



4. 構成管理の設定

Why / Risk

- いつ誰が何をしたか、はCloudTrailの証跡ログから追えるが、そのときAWSのリソースが**どういう状態**だったかわからない
 - 一応証跡ログを順番に追っていけば再現できなくはない... 😊
- 昨年の年末セール対応ってサーバ何台用意してましたっけ？
 - ドキュメントには20台ってあるけど、当日増やした気が...

Answer

- **AWS Config**の有効化
 - AWSリソースの状態や、各リソースのRelationship (関係) を記録
 - イベントの前後でAWSのリソースが**どう変化したか**記録
 - ルールを定義してルールに沿った設定がされているか自動チェック
 - すべてのAWSサービスの状態を記録してくれるわけではない ⚠

Break

- CloudTrailやAWS Configのログは延々と溜まり続ける
 - S3バケットのログはLifecycle機能で一定期間過ぎたら自動削除
 - CloudWatch Logsのログは保持期間の設定で自動削除
- AWS ConfigもCloudTrailと同じく外部サービスと連携して可視化
 - Splunk
 - Logstorage
 - CloudCheckr
 - 2ndWatch
 - etc...

<https://aws.amazon.com/jp/config/partners/>

1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
4. 構成管理の設定
5. Trusted Advisor
6. 請求周りの設定

Appendix. 複数のAWSアカウント運用Tips

5. Trusted Advisor

Why / Risk

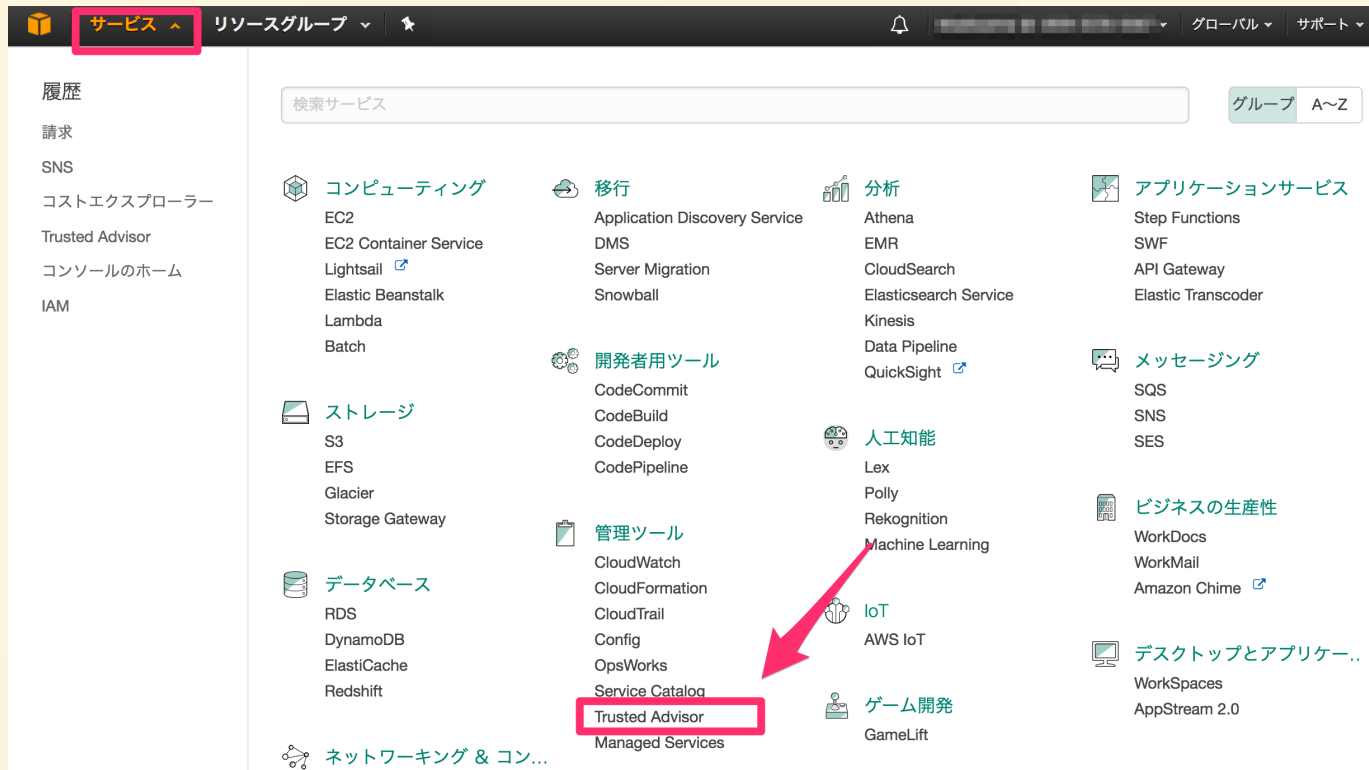
- 現状のAWS設定に危険な設定がないか不安 🙄
- 人手ではチェックしきれない、適切なチェックができない

Answer

- Trusted Advisorで以下の4項目を自動でチェックしてレコメンド
 - コスト最適化 (不要なリソースの発見など)
 - パフォーマンス (スペック不足やAWSの制限に達していないかなど)
 - セキュリティ (AWSサービスの権限設定や危険なポート許可など)
 - フォールトトレランス (冗長化やバックアップの設定など)
- Trusted Advisorは無料、サポートレベルによりチェック項目が増加

5. Trusted Advisor

左上の [サービス] から [Trusted Advisor] をクリック



5. Trusted Advisor

4項目がすべてグリーンになっているかチェック



Trusted Advisor ダッシュボード

コスト最適化	パフォーマンス	セキュリティ	フォールトトレランス
0 ✓ 0 ⚠ 0 !	1 ✓ 0 ⚠ 0 !	3 ✓ 0 ⚠ 0 !	0 ✓ 0 ⚠ 0 !

推奨されるアクション

- ▶ ✓ セキュリティグループ - 開かれたポート
更新済み: 5時間前
特定のポートに対して無制限アクセス(0.0.0.0/0)を許可しているセキュリティグループのルールをチェックします。
0個中0個のセキュリティグループのルールは、特定のポートに対して無制限アクセスを許可しています。
- ▶ ✓ IAM の使用
更新済み: 5時間前
この機能は、AWS Identity and Access Management (IAM)が使用されているかについてチェックします。
少なくとも一人の IAM ユーザーが作成されました。
- ▶ ✓ ルートアカウントのMFA
更新済み: 5時間前
このチェックではルートアカウントでMFAが有効にされていない場合にアラートを表示します。
このルートアカウントでは、MFAが有効にされています。
- ▶ ✓ サービス制限
更新済み: 5時間前

5. Trusted Advisor

先ほど作業したルートアカウントのMFAが有効でなかったり、EC2に対して不要だと思われるポートが許可されていると以下のように警告が表示される

Trusted Advisor ダッシュボード



コスト最適化	パフォーマンス	セキュリティ	フォールトトレランス
			
0  0  0 	1  0  0 	1  1  1 	0  0  0 

推奨されるアクション



セキュリティグループ - 開かれたポート

更新済み: 37分前

特定のポートに対して無制限アクセス(0.0.0.0/0)を許可しているセキュリティグループのルールをチェックします。

232個中92個のセキュリティグループのルールは、特定のポートに対して無制限アクセスを許可しています。





ルートアカウントのMFA

更新済み: 37分前

このチェックではルートアカウントでMFAが有効にされていない場合にアラートを表示します。

このルートアカウントでは、MFAが有効にされていません。

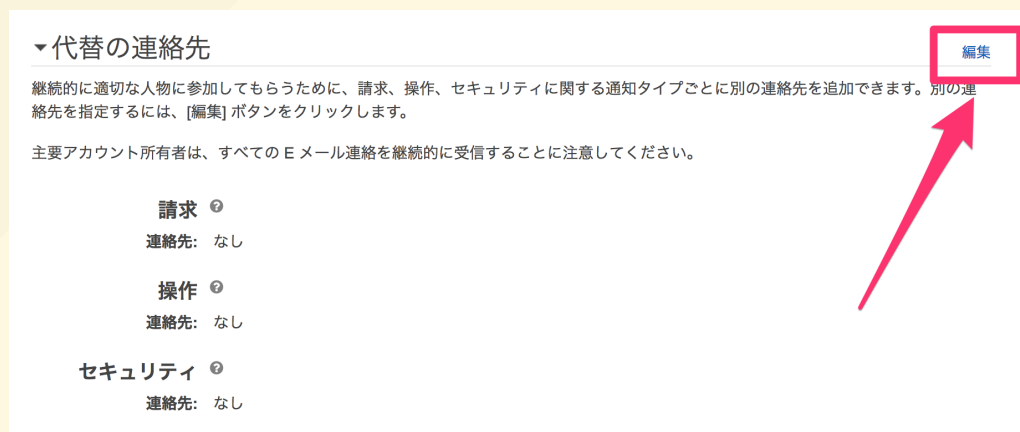


5. Trusted Advisor

[通知設定] から変化があった場合にメールでの通知を行うことができる



受信するメールアドレスを設定



5. Trusted Advisor

Why / Risk

- 現状のAWS設定に危険な設定がないか不安 🙄
- 人手ではチェックしきれない、適切なチェックができない

Answer

- Trusted Advisorで以下の4項目を自動でチェックしてレコメンド
 - コスト最適化 (不要なリソースの発見など)
 - パフォーマンス (スペック不足やAWSの制限に達していないかなど)
 - セキュリティ (AWSサービスの権限設定や危険なポート許可など)
 - フォールトトレランス (冗長化やバックアップの設定など)
- Trusted Advisorは無料、サポートレベルによりチェック項目が増加

Break

サポートレベルによりチェック項目が増加

- Basicプラン (Free)
チェック項目数**4個** (コスト最適化とフォールトトレランスはなし)



- Businessサポートの場合 (月額料金1割増し or \$100)
チェック項目数**55個**

<https://aws.amazon.com/jp/premiumsupport/trustedadvisor/best-practices/>



1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
4. 構成管理の設定
5. Trusted Advisor
6. 請求周りの設定

Appendix. 複数のAWSアカウント運用Tips

6. 請求周りの設定

Why / Risk

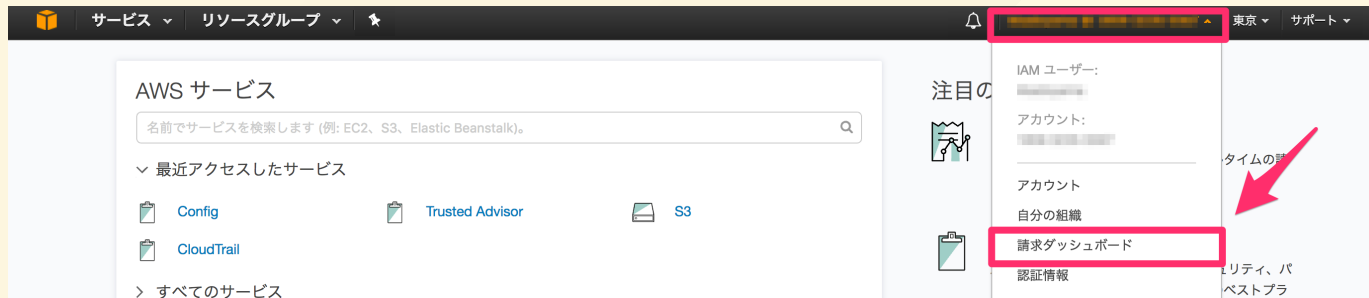
- デフォルトでは料金を見るのにルートアカウントが必要になる 🤔
- 気づかないうちにAWSの料金が**予算をオーバー**していた 😞 💰
- 意図していない支払いが発生していた 🔄 🔄 🔄

Answer

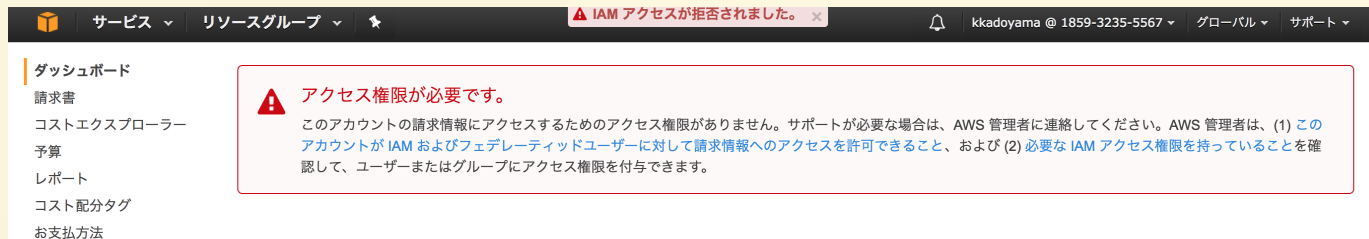
- IAMユーザーでも見れるようにする
 - 経理の方など請求周りの権限のみを持ったIAMユーザーの作成
- コストエクスプローラーにより料金の詳細な分析
- 毎月の実績や予測の予算を設定して、**超過しそうなら通知** 😊
- 毎月の料金をメールで受信する

6. 請求周りの設定 (IAM User)

メニューから [請求ダッシュボード] をクリック

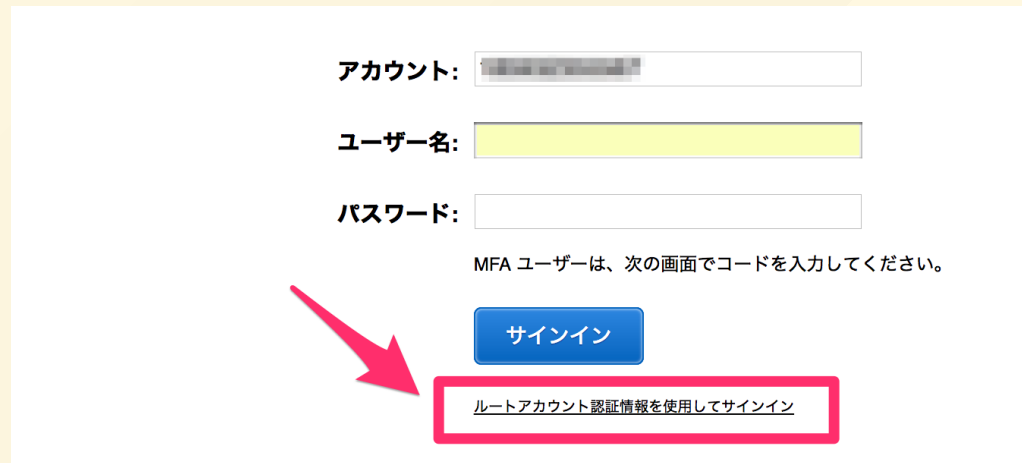


アクセス権限がないため拒否される



6. 請求周りの設定 (IAM User)

一度サインアウトし、ルートアカウントでサインインし直す



アカウント:

ユーザー名:

パスワード:

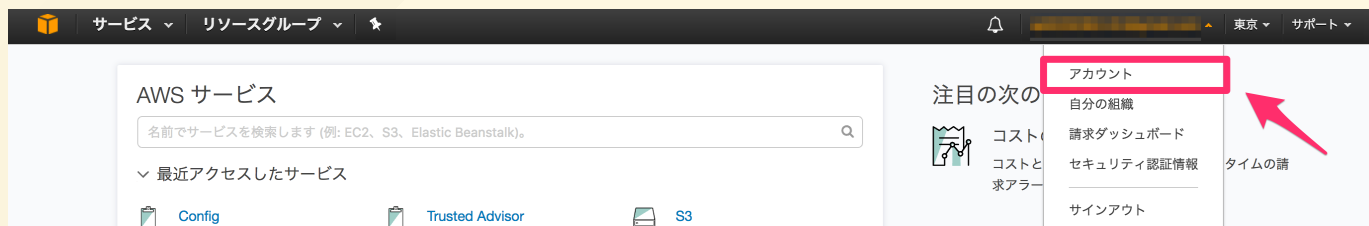
MFA ユーザーは、次の画面でコードを入力してください。

[サインイン](#)

[ルートアカウント認証情報を使用してサインイン](#)

A red arrow points from the 'サインイン' button to the link 'ルートアカウント認証情報を使用してサインイン', which is enclosed in a red rectangular box.

メニューから [アカウント] をクリック



6. 請求周りの設定 (IAM User)

[IAMユーザー/ロールによる請求情報へのアクセス] の編集をクリックし、

▼IAM ユーザー/ロールによる請求情報へのアクセス

編集

IAM ユーザーおよびフェデレーティッドユーザーに対して、請求情報にアクセスするためのロールのアクセス権限を付与できます。これには、アカウント設定、支払方法、およびレポートの各ページへのアクセスが含まれます。どのユーザーやロールに請求情報へのアクセスを許可するかは、IAM ポリシーを作成して制御できます。詳細については、「[請求情報へのアクセスコントロール](#)」を参照してください。

IAM ユーザー/ロールによる請求情報へのアクセスは無効になっています。

[IAMアクセスのアクティブ化] を設定

▼IAM ユーザー/ロールによる請求情報へのアクセス

IAM ユーザーおよびフェデレーティッドユーザーに対して、請求情報にアクセスするためのロールのアクセス権限を付与できます。これには、アカウント設定、支払方法、およびレポートの各ページへのアクセスが含まれます。どのユーザーやロールに請求情報へのアクセスを許可するかは、IAM ポリシーを作成して制御できます。詳細については、「[請求情報へのアクセスコントロール](#)」を参照してください。

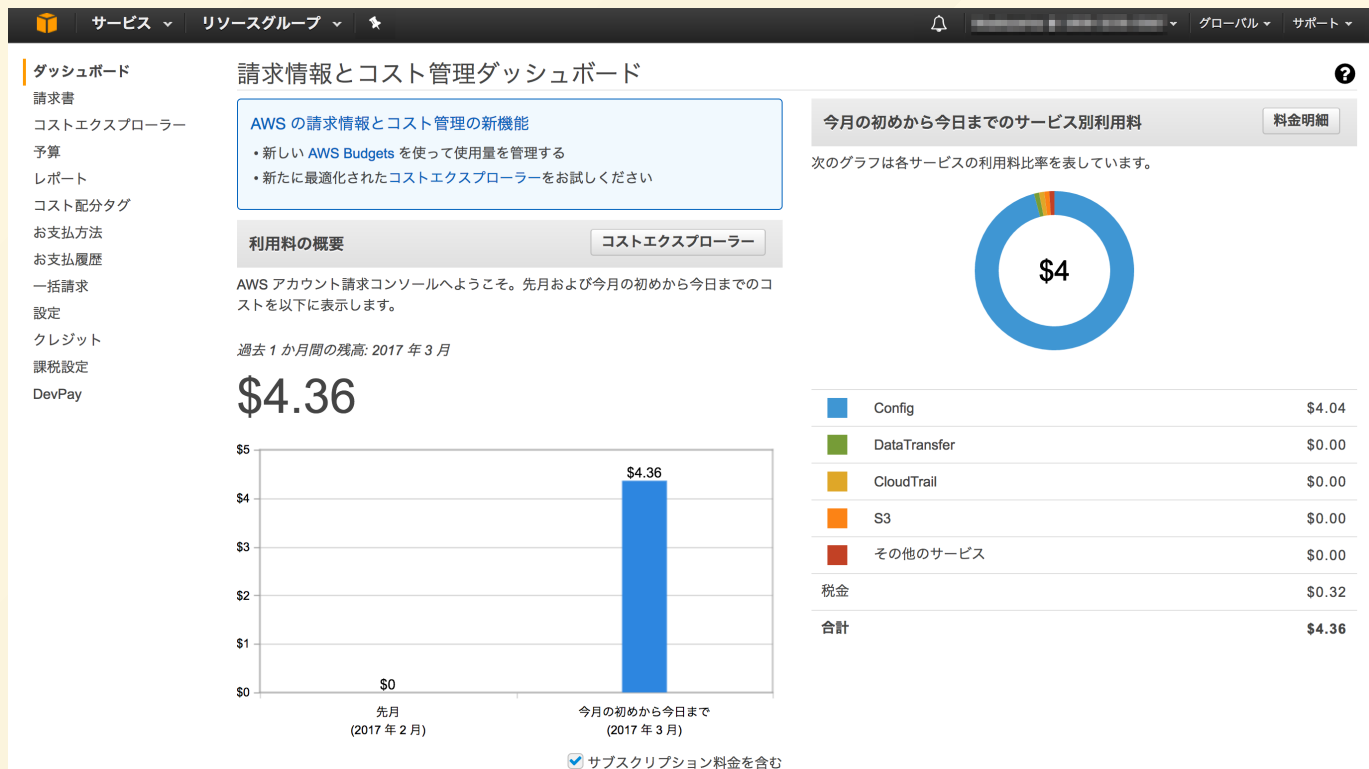
☒ IAM アクセスのアクティブ化

更新

 キャンセル

6. 請求周りの設定 (IAM User)

再度サインアウトしてIAMユーザーでサインインし直し、
メニューから [請求ダッシュボード] へアクセス



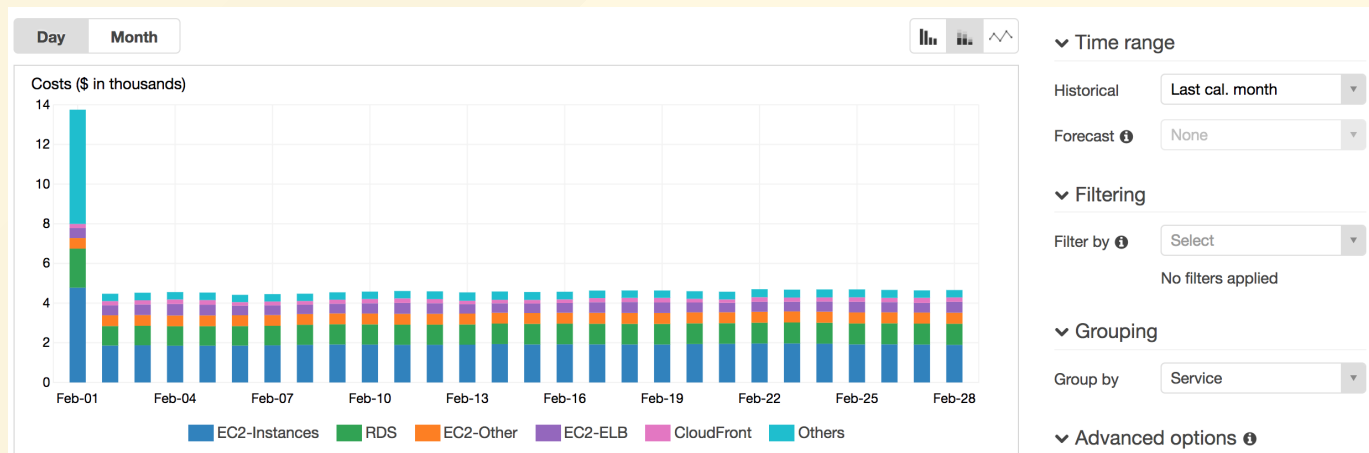
月のAWSサービス別の料金が表示される

6. 請求周りの設定 (CostExplorer)

コストエクスプローラー

コストエクスプローラーを使用すれば自由な分析が可能 (利用は無料)

- 日別／月別／年別の料金や推移
- 任意のタグでグルーピングした料金
- Consolidated Billingでまとめた各AWSアカウントの料金など



6. 請求周りの設定 (CostExplorer)

コストエクスプローラーの有効化

ダッシュボード
請求書
コストエクスプローラー
予算
レポート
コスト配分タグ
お支払方法
お支払履歴
一括請求
設定
クレジット
課税設定
DevPay

コストエクスプローラーへようこそ

コストエクスプローラーは、AWS のコストの追跡と管理に使用できるレポート、分析、可視化機能を提供します。

コストエクスプローラーを有効にしてから 24 時間以内に使用量データを見ることができるようになります。

コストエクスプローラーを有効化

機能の説明

構成済みのビューを使用する

サービスや連結アカウント別のコスト分布や、過去 3 か月の日別使用量を参照できます。

[詳細情報 »](#)

使用量を分析

コストエクスプローラーを使用して、過去の使用量を確認、分析します。

[詳細情報 »](#)

ダウンロードまたはブックマーク

レポートに関連付けられているデータをダウンロードするか、お気に入りのレポートをブックマークします。

[詳細情報 »](#)

6. 請求周りの設定 (Budgets)

予算

設定することで、料金が超過する／超過することが予想される場合などにアラートを送信することができる



The screenshot shows the AWS Budgets console interface. On the left sidebar, the '予算' (Budgets) menu item is highlighted with a red box. In the main content area, the 'AWS Budgets' header is visible, followed by a description of the service. Below this, a blue button labeled '予算を作成' (Create Budget) is highlighted with a red box and a red arrow pointing to it. The section titled 'AWS Budgets の開始方法' (How to get started with AWS Budgets) contains three steps: '予算の作成および管理' (Create and manage budgets), 'フィルタを使用して予算を絞り込む' (Narrow down budgets using filters), and '予算に通知を追加する' (Add notifications to budgets).

予算

ダッシュボード
請求書
コストエクスポージャー
予算
レポート
コスト配分タグ
お支払方法
お支払履歴
一括請求
設定
クレジット
課税設定
DevPay

AWS Budgets

AWS Budgets では、AWS のコストや使用量が設定値を超えたか、超えることが予想される場合に自動アラートを送信するカスタム予算を迅速に作成することができます。

予算を作成

AWS Budgets の開始方法



予算の作成および管理

AWS の使用量をより簡単に管理するために、カスタムコストと使用量の予算を設定します。予算ダッシュボードから予算の状況をモニタリングします。



フィルタを使用して予算を絞り込む

サービス、関連アカウント、アベイラビリティゾーンなどに関連するフィルタを追加して、複数のデイメンションでコストまたは使用量を追跡します。



予算に通知を追加する

メールを通じて通知を送信するか、通知を SNS トピックに発行して、設定値を超えたことを適切な人物に伝えます。

6. 請求周りの設定 (Budgets)

月別の予測コストが、指定した予算 (\$100) の80%を超過した場合にメールで通知

予算の作成

AWS コストあるいは使用量が設定したしきい値を超過した場合、あるいは超過すると予測された場合に、自動的にアラートするようにカスタム予算を作成します。

1 予算の詳細

名前* 月額AWS予算

コストまたは使用料を選択 コスト

間隔 月別

開始日 17/03/01

終了日 -

予算額* 100

2 含められる関連コスト

☐ サービス

☐ 関連アカウント

☐ タグ

☐ 購入オプション

☐ アベイラビリティゾーン

☐ API オペレーション

3 通知 (省略可能)

請求アラームを作成すると、現在のまたは予測されたAWSの料金が選択したしきい値に達したときに、メールアラートを受信できます。通知を受信するには、Eメール連絡先またはSNSトピックのARNを少なくとも1つ指定してください。

通知のタイミング: 予測 コスト > 80 % (予算額)

連絡電子メール [redacted]@gmail.com

SNS トピックの ARN 有効な SNS トピックの ARN を入力してください 検証

SNS トピックポリシーステートメント

+ 新しい通知の追加

* 必須

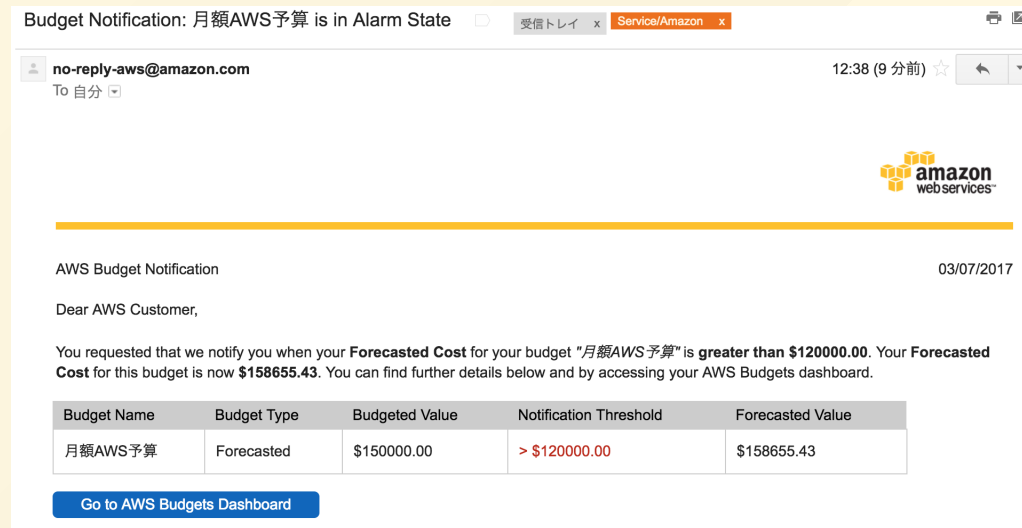
キャンセル 作成

AWS 予算の作成

- 1 予算に名前をつけ、予算額を指定し、予算が有効になる時間の長さを設定します。
- 2 オプションフィルターを選択して予算条件を絞り込みます。
- 3 予算のしきい値に達した場合に、EメールおよびSNSトピックで通知を送付します。

6. 請求周りの設定 (Budgets)

実際にAWSから送られてくるメール



6. 請求周りの設定 (Mail)

毎月の請求書 (PDF) をメールで受信する

ダッシュボード

請求書

コストエクスプローラー

予算

レポート

コスト配分タグ

お支払方法

お支払履歴

一括請求

設定

クレジット

課税設定

DevPay

設定

☒ 電子メールで PDF 版請求書を受け取る

PDF 版請求書を電子メールで受け取りたい場合は、このサービスをオンにしてください。請求書は、請求対象月の翌月 3 日頃に発行されます。

☐ 請求アラートを受け取る

AWS の利用料金と毎月発生する料金を自動的に監視する場合は、このサービスをオンにしてください。これにより、容易に AWS での使用料金を調べて管理することができます。請求アラートで、料金が設定した値に達したときにメール通知を受け取る様に設定することもできます。また請求アラートは一度オンにするとオフに戻す事はできません。[請求アラートを管理する](#) または、[新しい予算機能をお試しください!](#)

☐ 請求レポートを受け取る

AWS の料金に関する進行中のレポートを毎日 1 回以上に受け取るには、この機能をオンにします。下記で指定された S3 バケットにレポートが配信されます。レポートは支払アカウントに対してのみ配信されます。連結アカウントでは請求レポートを受け取ることができません。

S3 バケットに保存:

6. 請求周りの設定

Why / Risk

- デフォルトでは料金を見るのにルートアカウントが必要になる 🤔
- 気づかないうちにAWSの料金が予算をオーバーしていた 😞 💰
- 意図していない支払いが発生していた 🔄 🔄 🔄

Answer

- IAMユーザーでも見れるようにする
 - 経理の方など請求周りの権限のみを持ったIAMユーザーの作成
- コストエクスプローラーにより料金の詳細な分析
- 毎月の実績や予測の予算を設定して、超過しそうなら通知 😊
- 毎月の料金をメールで受信する

Break

アカウントや請求周りは他にもこんな設定が

- 支払い通貨の変更 (\$ → ¥)
 - クレカの手数料込みのレート or AWSのレート
- 秘密の質問の設定による本人確認の強化
- AWSからのマーケティングメールの受信設定
- 時間別の詳細料金レポートをS3にcsv出力



自分の組織／環境にあわせて適切な設定を

まとめ

- AWSアカウントを取得したら、MFAの設定やIAMユーザーの利用、証跡ログの記録など要件にあわせて初期設定をしておきましょう
※本番環境はとくに注意
- 設定しない場合でも、どういうリスクがあるかは把握しておきましょう
- AWSアカウントやコストの管理は自己責任 (ユーザー責任) です 🤔
- 予算超過のアラートやコストエクスプローラー、Trusted Advisorなど無料で利用できる便利なサービスが揃っています
- 夜も眠れない場合はAWSサポートやSAの方に相談を 😊

Wrap up

使用したリソースの削除

- 作成したCloudTrail、AWS Configの削除
- S3バケット、SNSのトピックの削除
- 作成したIAMユーザー、IAMグループの削除

Thanks!! & Questions?

本セッションの内容は以上です

お疲れ様でした

このあとも[JAWS DAYS 2017](#)をお楽しみください






1. ルートアカウントの保護
2. IAMユーザーとパスワードポリシー
3. 証跡ログの設定
4. 構成管理の設定
5. Trusted Advisor
6. 請求周りの設定


Appendix. 複数のAWSアカウント運用Tips

Apx. 複数のAWSアカウント運用

Why / Risk

- システム／環境が増えればAWSアカウントも増える
 - AWSのサービス制限の中にはアカウント単位のものもある
- ログイン用のIAMユーザー 
 - システム数 x 環境数 x 担当者数 = 
- アカウントごとに請求されることで請求処理の手間 

Answer

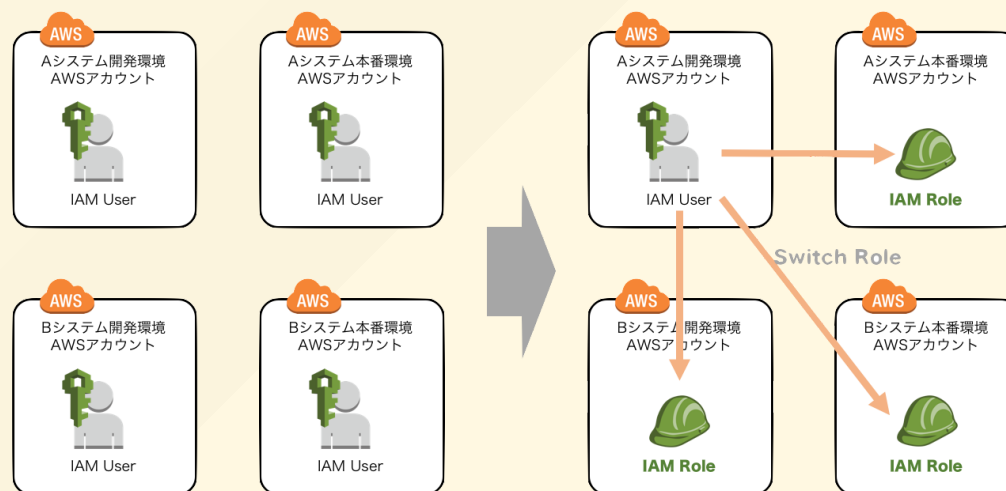
- 担当者につきIAMユーザーは1つで複数のAWSアカウントにログイン
 - Switch RoleによるAWSアカウント切り替え 
- 複数AWSアカウントの請求を1つにまとめる
 - Consolidated Billing (一括請求)

Apx. 複数のAWSアカウント運用

Switch Role

IAMユーザー = ログインやAPIでのアクセスに使用

IAMロール = IAMポリシー(権限)が付与された役割



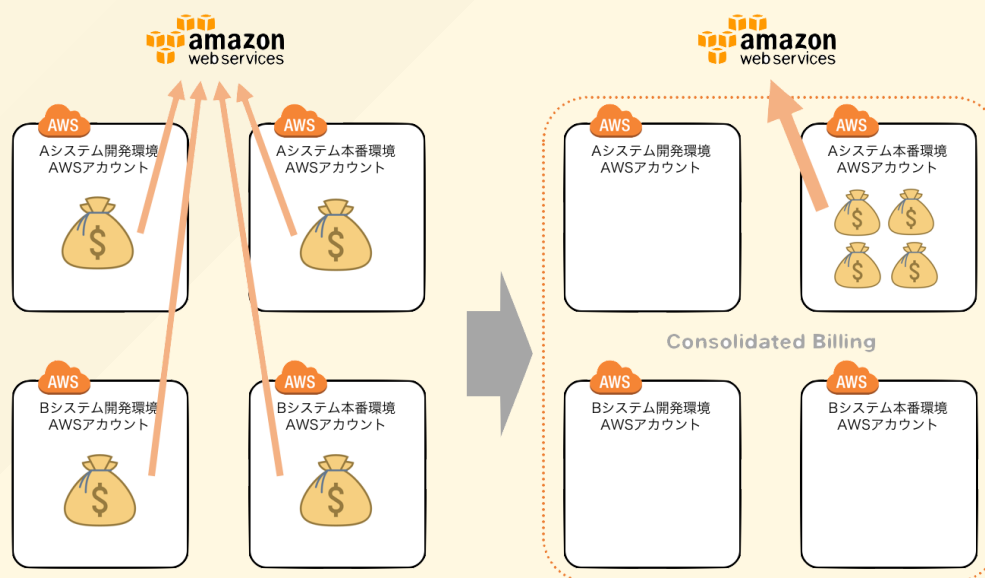
- AWSアカウントが4つある場合、そのまま利用すると利用者1人につきログイン用のIAMユーザーが4つ必要になる
- Switch Roleを使用すると、3つのAWSアカウントに切り替え用のIAMロールを作成し、利用者1人につきログイン用のIAMユーザーは1つですむ

Apx. 複数のAWSアカウント運用

Consolidated Billing

実際に請求がくる親アカウント1つと、
支払いをしてもらう子アカウント複数、
Consolidated Billingアカウントファミリーとして紐付ける
支払いは親アカウントからまとめておこなわれる

https://docs.aws.amazon.com/ja_jp/awsaccountbilling/latest/aboutv2/consolidated-billing.html



ボリューム割引やファミリー間のReserved Instances共有などのメリットも 91

Apx. 複数のAWSアカウント運用

AWS Organizations

<https://aws.amazon.com/jp/about-aws/whats-new/2017/02/aws-organizations-now-generally-available/>

メニュー



開始方法

製品 ▾

ソリューション

料金表

ソフトウェア

詳細 ▾

日本語 ▾

アカウント ▾

サインアップ

AWS について

AWS について >

グローバルインフラストラクチャ >

最新情報 >

AWS メディア掲載記事 >

国内のセミナー・イベントスケジュール >

関連リンク

クラウドとは？

クラウドの強みとメリット

AWS クラウド 無料利用枠

AWS Organizations が一般公開されました

上の投稿: Feb 27, 2017

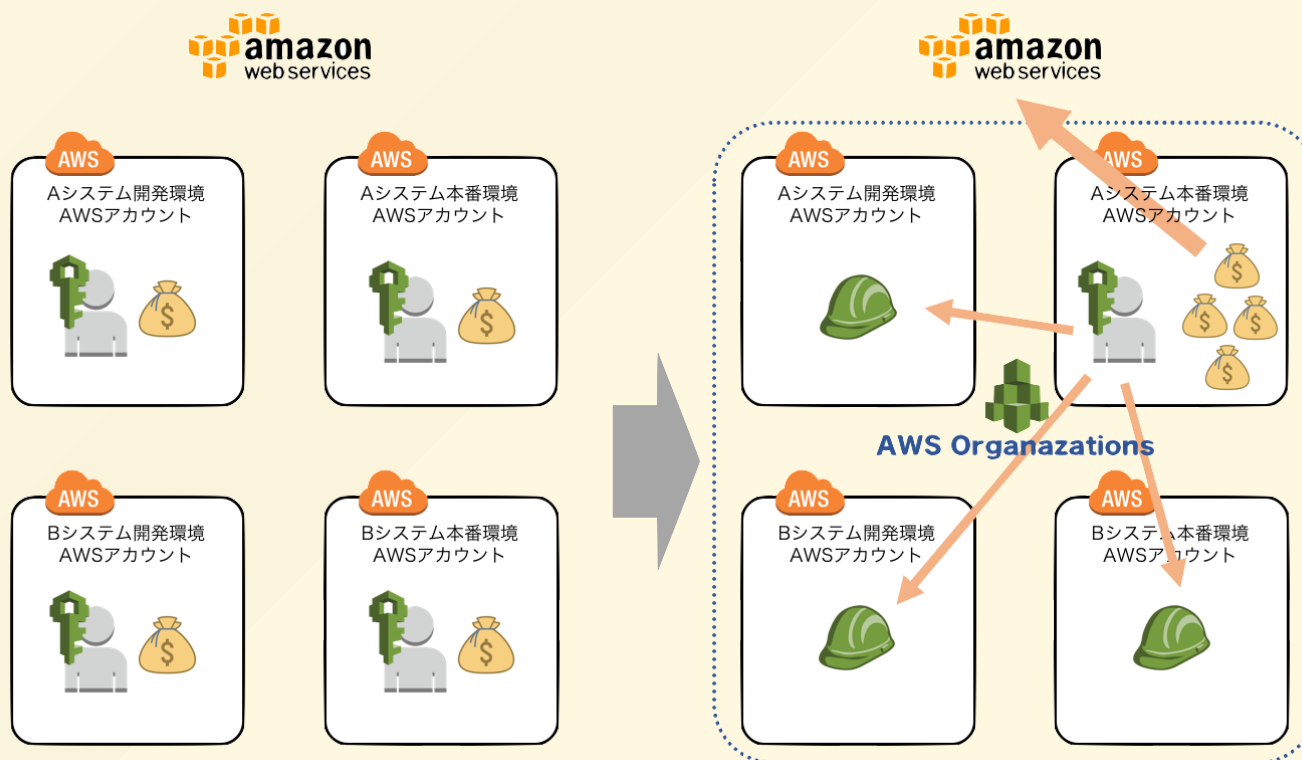
AWS Organizations は、複数の AWS アカウントのポリシーベースの管理を提供するもので、すべてのお客様向けに一般公開されました。Organizations を使用すると、アカウントのグループを作成し、それらのグループにポリシーを適用できます。Organizations により、カスタムスクリプトや手動のプロセスを必要とすることなく、複数のアカウントでポリシーを一元管理することができます。

AWS Organizations を使用すると、複数の AWS アカウントでの AWS のサービスの使用を一元管理する Service Control Policies (SCP) を作成できます。また、API を通じた新しいアカウントの作成を自動化するうえで役立ちます。Organizations では、一括請求 (コンソリデेटッドビルディング) を通じて組織のすべてのアカウントに対する単一の支払い方法をセットアップ可能にして、複数のアカウントに対する請求を簡略化できます。

AWS Organizations は追加料金なしで、中国 (北京) および [AWS GovCloud \(US\)](#) を除くすべての AWS リージョンでご利用いただけます。Organizations のサービスエンドポイントは米国東部 (バージニア北部) にありますが、SCP は利用可能なすべてのリージョンに適用されます。[Organizations の製品ページ](#)で Organizations の詳細を参照し、今すぐ無料でサインアップしてください。

Apx. 複数のAWSアカウント運用

- Consolidated Billing + 複数AWSアカウントを管理
- ポリシーを適用することで利用できるAWSリソースを機能を制限



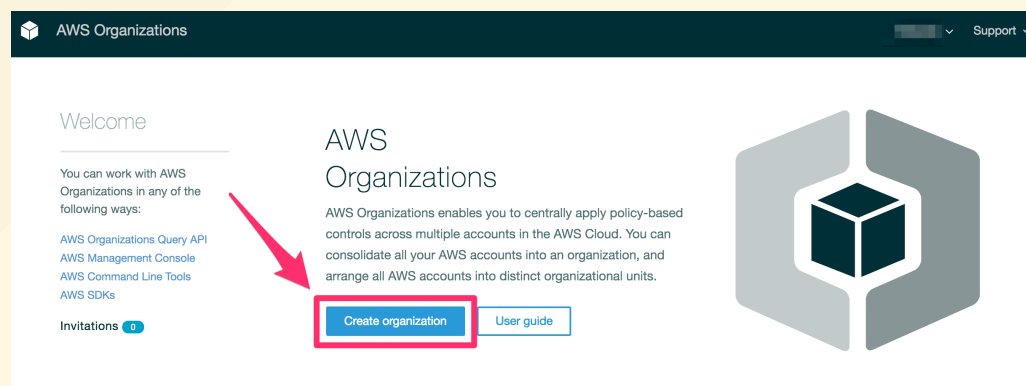
Apx. 複数のAWSアカウント運用

以下のURLにアクセスし、[使用を開始する]

<https://aws.amazon.com/jp/organizations/>

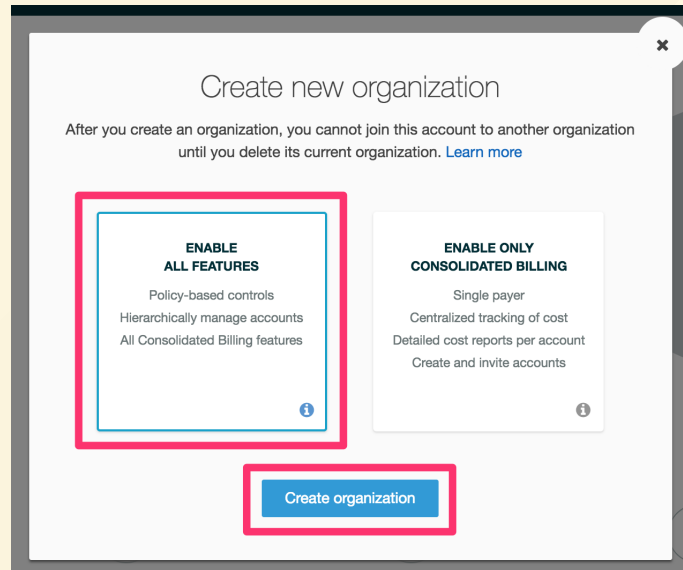


[Create Organization] をクリック



Apx. 複数のAWSアカウント運用

[ENABLE ALL FEATURES] をクリック

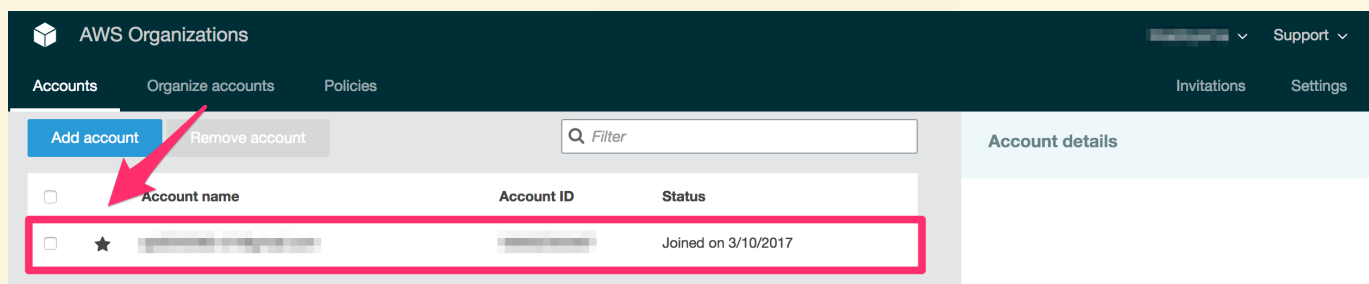


- ENABLE ONLY CONSOLIDATED BILLING
 - これまでのConsolidated Billingのみの機能、請求をまとめるだけ
- ENABLE ALL FEATURES
 - 上記に加え、ポリシーによる権限管理や今後実装されるであろう機能が利用可能

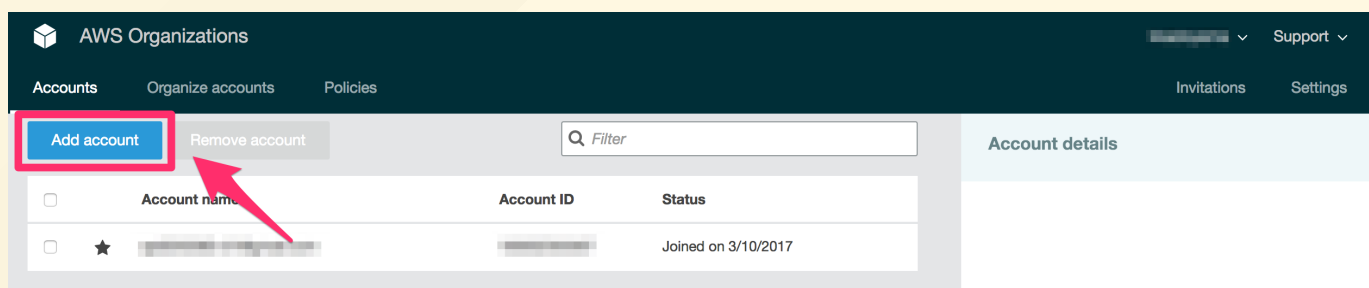
Apx. 複数のAWSアカウント運用

★ マスターアカウントになる

※Consolidated Billingという親アカウント (実際に請求がくる)

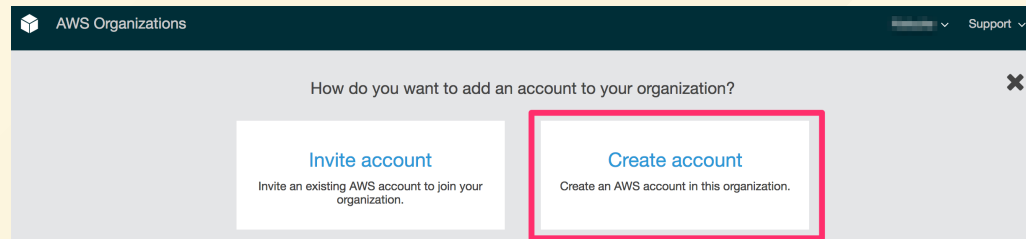


左上の [Add account] からAWSアカウントを追加

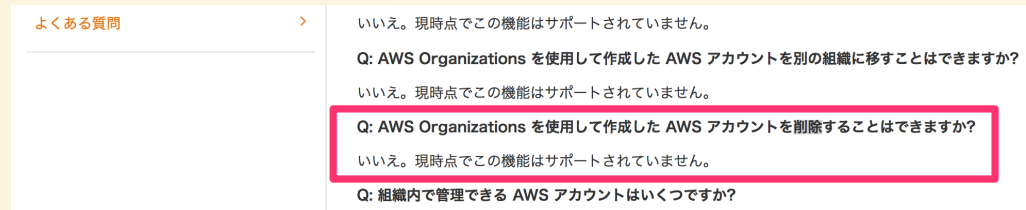


Apx. 複数のAWSアカウント運用

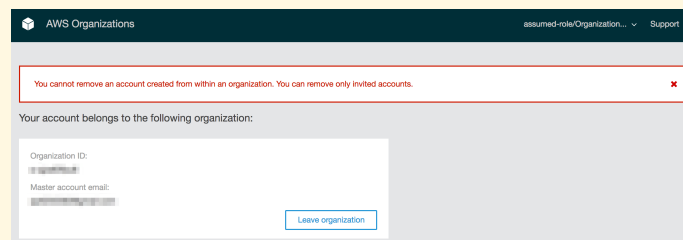
[Create account] からAWSアカウントを新規作成



[Create account] で新規作成したAWSアカウントは現状削除できない
ただし解約はできる、、、AWS Organizations上から消せないだけ 🤔



[Remove account] しようとしても。 🤔



Apx. 複数のAWSアカウント運用

- ①[Full name] はAWSアカウント名
- ②[Email] はAWSアカウントを作成する際に入力するメールアドレスで一意
※ハンズオンの最初で作成したメールアドレスとは異なるものを設定
- ③[IAM role name] は作成するAWSアカウントに用意されるIAMロール名
※未指定だと [OrganizationAccountAccessRole] になる

AWS Organizations

kkadoyama ▾ Support ▾

How do you want to add an account to your organization? ✕

Invite account
Invite an existing AWS account to join your organization.

Create account
Create an AWS account in this organization.

Full name* ①

Email* ②

IAM role name ③

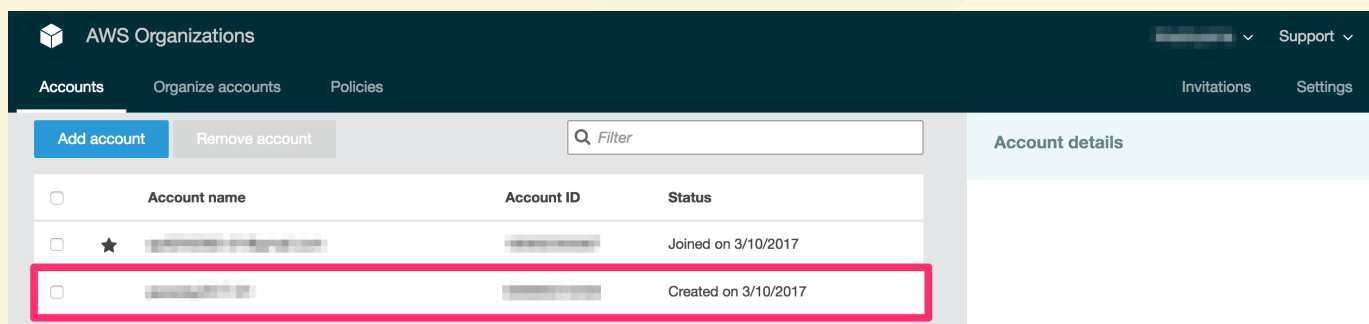
This account is created using the contact information address of the organization's master account.

* Required fields

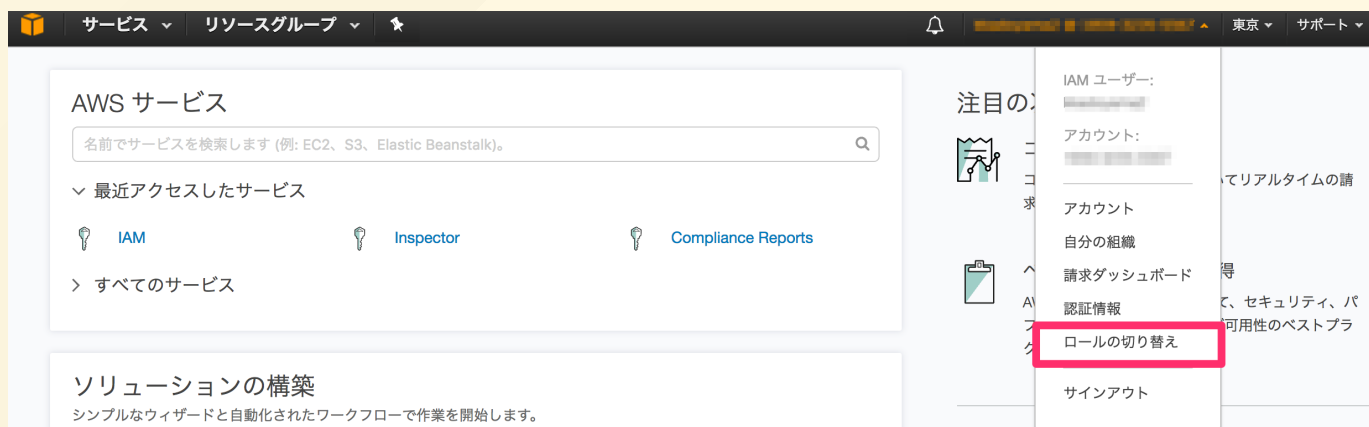
Apx. 複数のAWSアカウント運用

AWSアカウントの追加が完了

※追加されたAWSアカウントの [Account ID] をメモ



右上のIAMユーザー名をクリックし [ロールの切り替え]



Apx. 複数のAWSアカウント運用

- ①[アカウント] には先ほどメモした作成したAWSアカウントの
[Account ID (12桁数字)] を入力
- ②[ロール] には作成したAWSアカウントのIAMロール名を入力
※作成時に未指定の場合は [OrganizationAccountAccessRole]
- ③[表示名] はエイリアスなのでお好みで

ロールの切り替え

単一ユーザー ID とパスワードを使用している AWS アカウント全体にわたって、リソースの管理を許可します。AWS 管理者がロールを設定してアカウントとロールの詳細が提供されると、ロールを切り替えることができます。 [詳細はこちら](#)。

アカウント* ⓘ ①

ロール* ⓘ ②

表示名 ⓘ ③

色 a a a a a a

*必須

キャンセル

ロールの切り替え

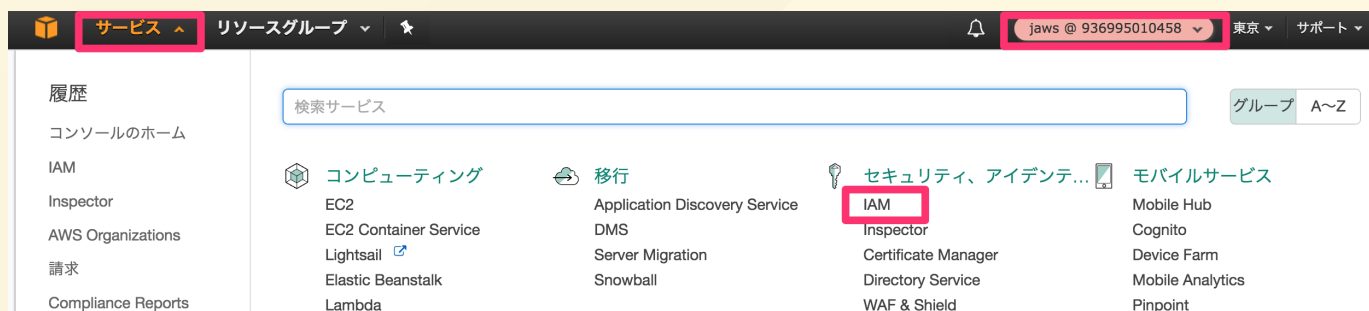
Apx. 複数のAWSアカウント運用

AWSアカウントが切り替わる

右上のアカウント名が [IAMロール名]@[Account ID] になる

※ロールの切り替えで [表示名] を設定した場合は [表示名] が表示

左上の [サービス] から [IAM] をクリック



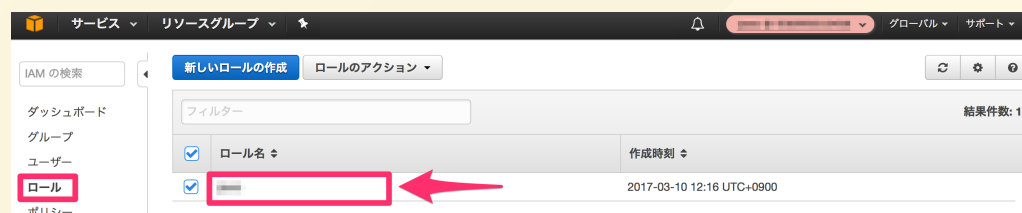
初期状態のIAMの画面が表示



Apx. 複数のAWSアカウント運用

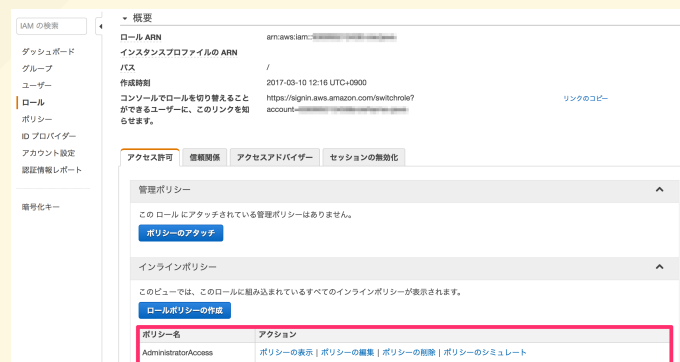
左メニューから [ロール] をクリック

AWS OrganizationsからAWSアカウント作成の際に指定したIAMロールが表示されるので、ロール名をクリック



[AdministratorAccess] ポリシーが設定されている

今後はこのIAMロールを起点に、必要な役割分のIAMロールを作成してマスターアカウントに作成したIAMユーザーから切り替えて利用

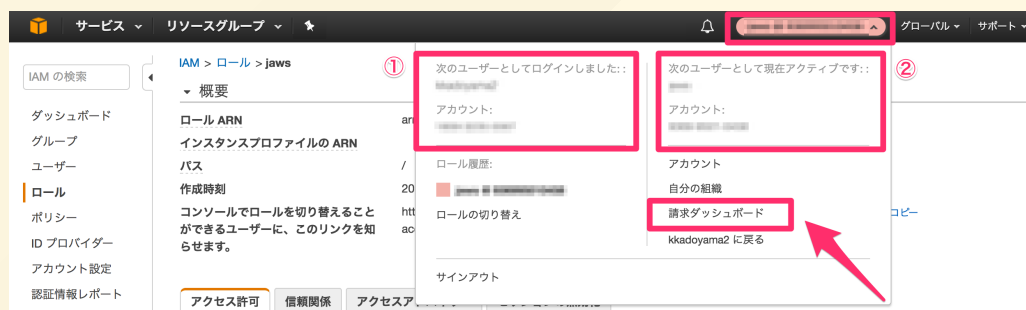


Apx. 複数のAWSアカウント運用

右上のアカウント名をクリック

- ①がAWSコンソールにログインしたIAMユーザーとAWSアカウントの情報
- ②が現在操作中の切り替えた先のIAMロールとAWSアカウントの情報

[請求ダッシュボード] をクリック



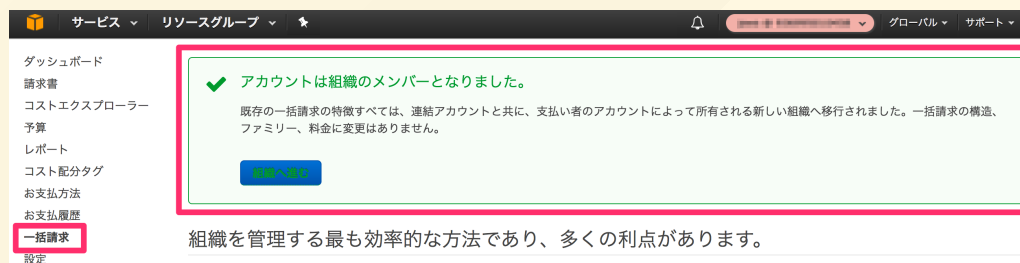
最初から料金が見える状態になっている (P76の設定不要)



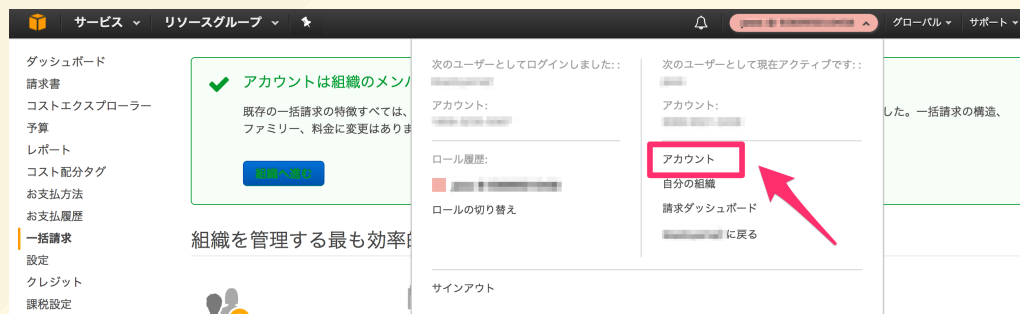
Apx. 複数のAWSアカウント運用

左メニューから [一括請求] をクリック

AWS Organizationsのメンバーで、料金請求はマスターアカウントにまとめられている

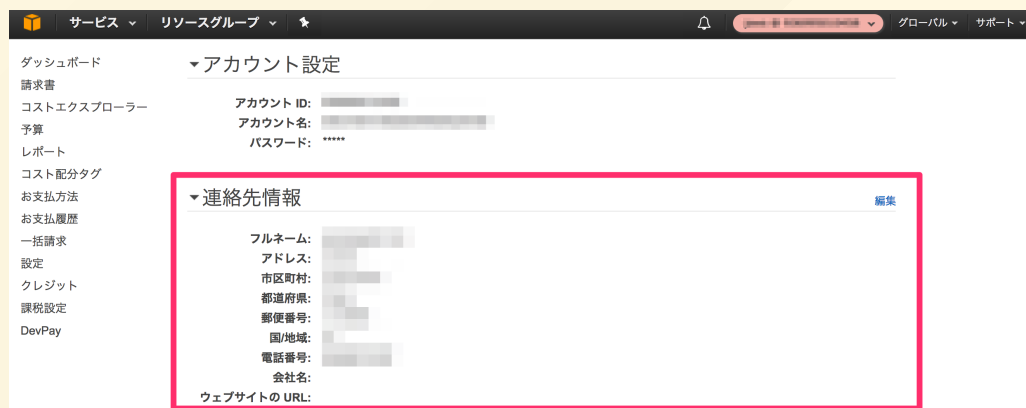


右上のアカウント名クリックから [アカウント] へ



Apx. 複数のAWSアカウント運用

AWSアカウントの住所など連絡先はマスターアカウントと同じものが設定されている






右上のアカウント名クリックから [xxx (IAMユーザー名) に戻る] で切り替え元のAWSアカウントに戻る

※ハンズオンでは最初にIAMユーザーを作成したAWSアカウントに戻る




Apx. 複数のAWSアカウント運用

Why / Risk

- システム／環境が増えればAWSアカウントも増える
 - AWSのサービス制限の中にはアカウント単位のものもある
- ログイン用のIAMユーザー  
 - システム数 x 環境数 x 担当者数 = 
- アカウントごとに請求されることで請求処理の手間

Answer

- AWS Organizationsを利用してAWSアカウントを一元管理
 - 担当者につきIAMユーザーは1つで複数のAWSアカウントにログイン
 - Switch RoleによるAWSアカウント切り替え 
 - 複数AWSアカウントの請求を1つにまとめる

Break

AWS Organazations Tips (1/2)

- ポリシー (Service Control Policies: SCPs) により、各AWSアカウントで利用できるAWSサービスとオペレーションを制限できる
 - 例えばEC2とS3のみ利用可能だがEC2のTerminateは禁止、など
 - システムに必要なAWSサービスのみ制限したり、本番環境で不要なAWSサービス作成を制限したり
 - AWS OrganazationsのポリシーとIAMポリシーによる両方の制限



- OUという組織単位でAWSアカウントをグルーピング&階層構造で管理
 - ポリシーをOUに設定して配下のOU/AWSアカウントすべてに適用

Break

AWS Organazations Tips (2/2)

- AWS OrganazationsからAWSアカウントを作成した場合のルートアカウントは？
 - 存在するがパスワード未設定の状態になっている
 - サインイン時の [Forgot your password?] からパスワードを設定すれば使えるようになる

Sign In or Create an AWS Account

What is your email (phone for mobile accounts)?

E-mail or mobile number:

☐ I am a new user.

☒ I am a returning user and my password is:

Sign in using our secure server

[Forgot your password?](#)

EC2-Mail送信制限緩和や侵入テスト申請など、
どうしてもルートアカウントが必要な場面で

EOF